

Virtual Native Network®

VNN4 客户端用户使用手册

IMPORTANT NOTICE

No portion of VNN Software or any of its subparts may be reproduced in any form, or by any means, without prior written permission from VNN Networks, Inc.

VNN Networks, Inc. and its subsidiaries reserve the right to make changes to their datasheets and/or products or to discontinue any product or service without notice, and advise customers to obtain the latest version of relevant information to verify, before placing orders, that information being relied on is current and complete. All products are sold subject to the terms and conditions of sale supplied at the time of order acknowledgement, including those pertaining to warranty, patent infringement, and limitation of liability.

VNN Networks, Inc. warrants performance of its products to the specifications applicable at the time of sale in accordance with VNN Networks, Inc.'s standard warranty. Testing and other quality control techniques are utilized to the extent VNN Networks, Inc. deems necessary to support this warranty. Specific testing of all parameters of each device is not necessarily performed, except those mandated by government requirements.

Customer acknowledges that VNN products are not designed, manufactured or intended for incorporation into any systems or products intended for use in connection with life support or other hazardous activities or environments in which the failure of the VNN products could lead to death, bodily injury, or property or environmental damage ("High Risk Activities"). VNN Networks, Inc. hereby disclaims all warranties, and VNN Networks, Inc. will have no liability to Customer or any third party, relating to the use of VNN products in connection with any High Risk Activities.

Any support, assistance, recommendation or information (collectively, "Support") that VNN may provide to you (including, without limitation, regarding the design, development or debugging of your application) is provided "AS IS." VNN Networks, Inc. does not make, and hereby disclaims, any warranties regarding any such Support, including, without limitation, any warranties of merchantability or fitness for a particular purpose, and any warranty that such Support will be accurate or error free or that your application will be operational or functional. VNN Networks, Inc. will have no liability to you under any legal theory in connection with your use of or reliance on such Support.

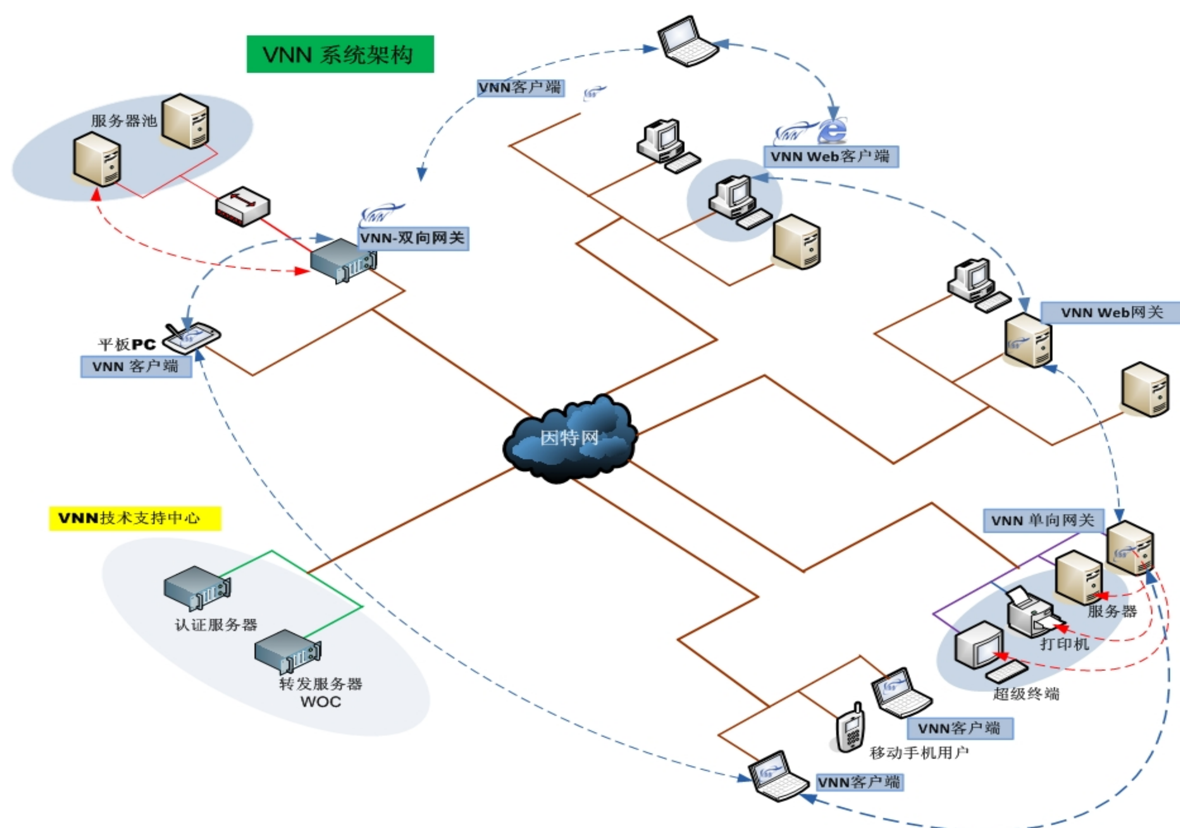
目录

Chapter 1

系统简介

VNN Enterprise 4 是一款完成企业局域网互联互通的网络通讯产品，是提供远程访问的安全解决方案。通过 VNN，无需公网 IP 地址，无需改动任何企业内部的网络配置，家庭办公用户、移动办公用户和合作伙伴等即可轻松安全地访问企业内部网。

VNN 通过对用户的认证，基于角色的访问控制以及数据加密技术为用户提供了安全保障。而且支持广泛的基于 TCP/UDP 的多种应用，如 FTP 、TFTP、Telnet、终端服务器、VNC、文件共享、SSH、HTTPS、Oracle 、Exchange/Outlook、Lotus Notes 等。VNN 内置的加密算法和压缩算法，使数据在 VNN 的虚拟网上传送既安全又快速。



Chapter 1

1.1 典型部署方式

VNN 有两种典型部署方式：直连模式、网关模式。网关模式又分为 PPTP 模式和 NAT 模式。可参见下面的 VNN 典型布局结构图示。

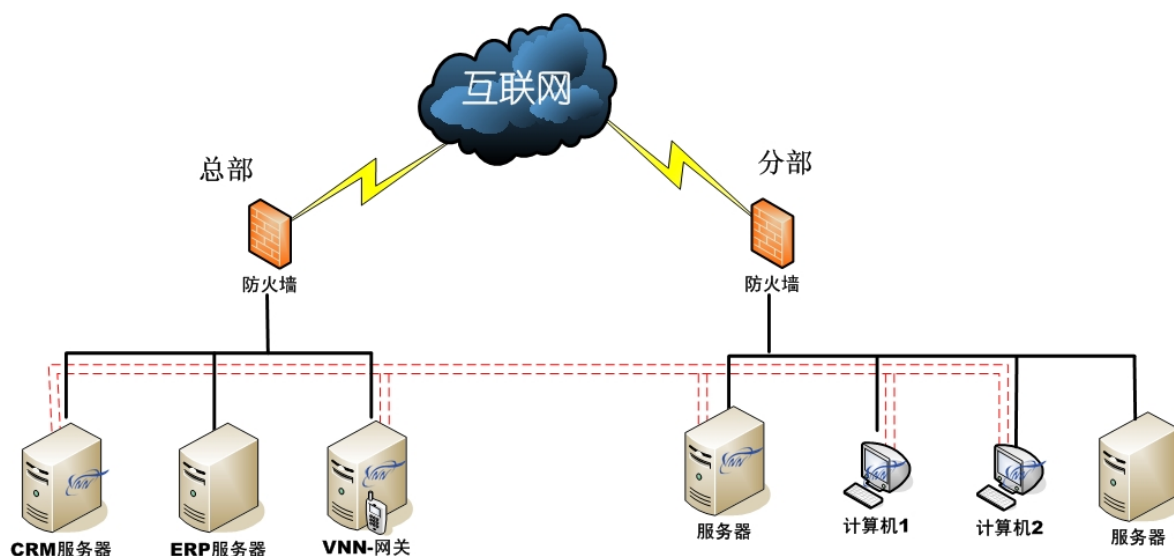
直连模式：VNN Enerprise 4 客户端软件直接部署在企业内网的计算机上。客户端之间传送数据为点到点的直接传输模式，不经过任何服务器转发，传输数据速度最快的模式。

VNN 网关 PPTP 模式：VNN Enterprise 4 客户端软件部署在企业内网的一台计算机上，为在局域网里无法安装 VNN 客户端的主机或者 IP 设备提供一个进入 VNN 网络的入口。VNN 网关分配 VNN 网关中的子网 IP 给这些客户端，客户端通过 PPTP 的方式拨号到 VNN 网关以进入 VNN 网络。

VNN 网关 NAT 模式：VNN Enterprise 4 客户端软件部署在企业内网的一台计算机上，为在局域网里无法安装 VNN 客户端的主机或者 IP 设备提供一个被 VNN 网络里的计算机访问到的方式。VNN 网关通过映射 VNN 的 IP 地址到客户端所在的局域网中的计算机或设备的物理（内网或公网）IP 地址，使访问 VNN 网络里面的计算机可以访问到这些远程的计算机或设备。

VNN 直连模式（下图）

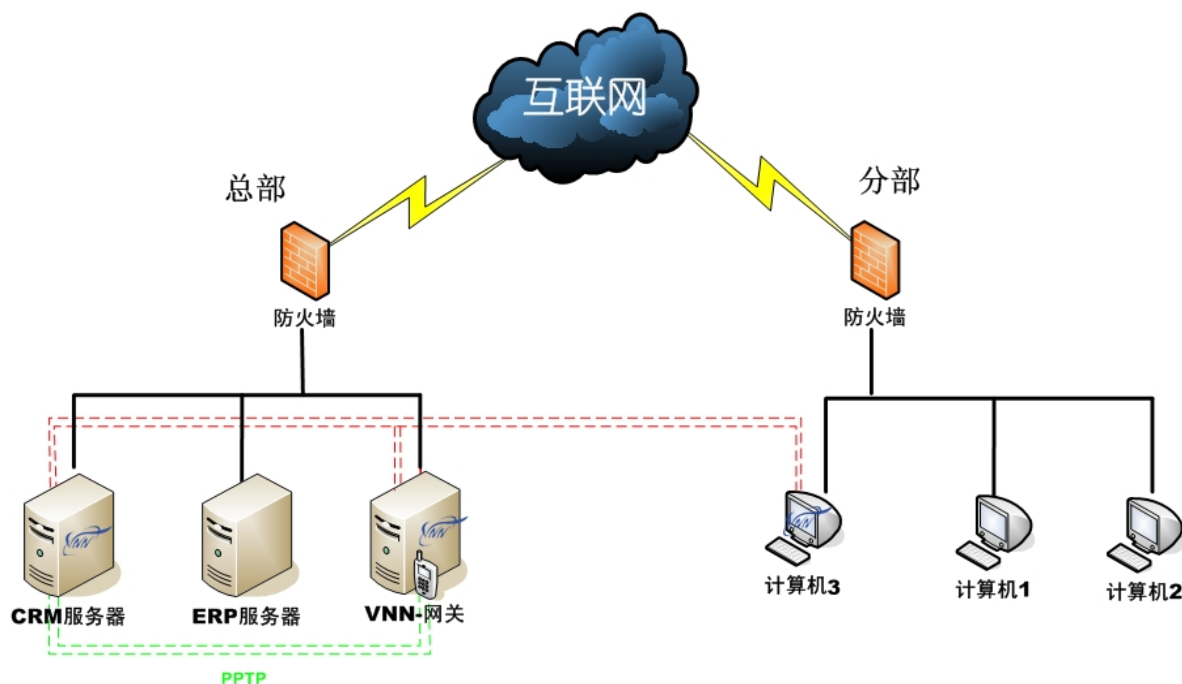
带有 VNN Logo 图标的设备为安装了 VNN 客户端软件的设备，所有安装了 VNN 客户端软件的设备都可以互相访问。



Chapter 1

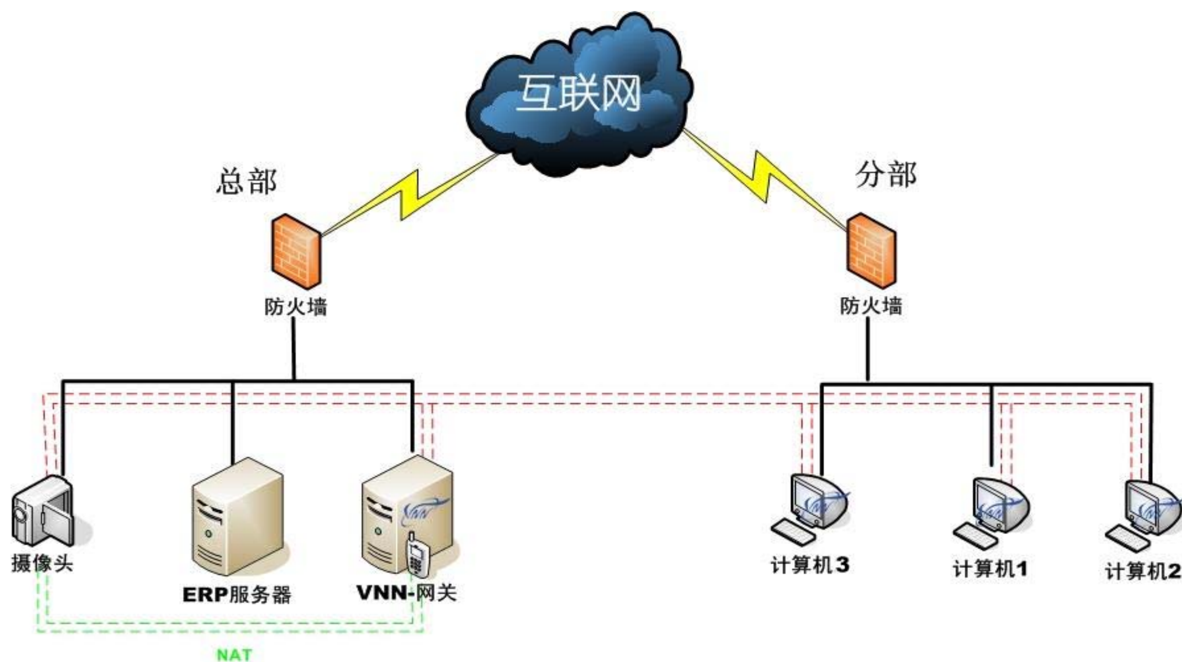
VNN 网关 PPTP 模式（下图）

CRM 服务器(未接入互联网)通过 PPTP 程序拨号到了同一局域网中 VNN 网关,从而加入了 VNN 的虚拟网络，组成了虚拟局域网并同计算机 3 通信。



VNN 网关 NAT 模式（下图）

VNN 网关映射网关子网 IP 到无线摄像头所获得的物理 IP，这样远程的计算机 1，计算机 2，计算机 3 就可以通过访问 VNN 网关子网 IP 地址来访问无线摄像头。



1.2 系统需求

操作系统：

Windows 2000 SP4 及以上，32 位 Windows XP 及以上，64 位 Windows XP 及以上，32 位 Windows Vista，64 位 Windows Vista，32 位 Windows 2008，64 位 Windows 2008。如果使用网关版本，则网关后面的机器，任意支持建立 PPTP 拨号的操作系统（Unix, Linux, Mac, Sybian 等）都可以。

网络：

需要能够访问互联网，并且防火墙没有阻止 VNN 所使用的 TCP 和 UDP 端口。对于网速，没有特别要求，无论是拨号还是 ADSL 或者小区宽带、城市光纤、CDMA、无线宽带等，VNN 都支持。

1.3 系统主界面

下图为 VNN 程序的主界面：



Chapter 1

1.4 系统主界面选项



❶ 点击“在线客服”可获得 VNN 技术支持人员在线支持。点击“登录”按钮可以返回到登录界面，点击“工具”按钮进入 VNN 高级功能设置（详情请见 2.8.3）。

❷ 帐号格式为***.组名.vnn，输入帐号密码点击“登录”即可登陆 VNN 并获得 VNNIP，如不想在登录 VNN 时每次都输入密码并点击登录来上线，可以勾选上“记住输入的密码”和“自动上线”复选框。

❸ 点击“注册”按钮，您可以注册一个 VNN 组。

❹ VNN 的版本号。

Chapter 2

系统设置

本章将详细介绍 VNN 组的注册及使用。

2.1 系统>>注册新组

当 VNN 安装完毕后，用户需要通过创建一个组和至少 2 名组成员帐号以便进行加密通信。

双击桌面上的“VNN-Enterprise Console”图标打开 VNN 的登录界面，通常在安装完 VNN 后该界面会自动打开。在界面载入完毕后，可以在登录窗口处看到一个“注册”按钮，点击该按钮以继续。

在出现的申请新组的界面中，在“组名”文本框中输入一个符合用户要求的组名，该组名必须大于 3 个字符，小于 32 个字符，同时必须为半角英文或数字。在“邮件”文本框中输入一个真实的邮件地址以便于密码找回。输入您的 QQ 号码，便于技术人员支持。勾选需要的应用后选下一步。

当填写完信息后，点击下一步按钮继续。

当界面提示“你申请的组已经创建成功”后，VNN 会自动登录刚才创建的组的组管理员帐号，通常情况下该帐号是以 admin. 作为起始名称。同时，该帐号只能进行组管理，不能进行实际通信使用。

※注意：如果在以上步骤点击“下一步”时提示“组名已存在”则代表该组名已经被人注册。您需要使用一个其他的组名进行注册。

当登录成功后，VNN 会为该管理员帐号生成一个随机的密码，并且要求用户立即更改密码。新密码不能超过 31 位。输入完一个新的密码并确认后。

点击下一步按钮继续。

当密码修改成功后，注册向导会指导用户创建两个组成员。由于 VNN 是一个加密网络，因此用户双方都必须安装 VNN 并登陆相应的用户组成员的帐号才能够互相通信。因此至少需要两个帐号。

帐号的长度必须大于 2 位，小于 16 位，只能是半角英文字符或数字。

※注意：在此步骤中如果不想使用默认创建的帐号和密码，可选择手工创建帐号。

点击下一步按钮，VNN 注册向导会自动创建两个帐号并登录所创建的第一个帐号。



此时，只需要在另一台计算机上安装 VNN 并且登录第二个帐号，即可完成一个小型的虚拟局域网的组建。

2.2 系统>>注册新成员帐号

如果用户需要注册第三个或更多的帐号，则需要使用管理员帐号登录 VNN 进行添加操作。

首先，双击桌面上的“VNN-Enterprise Console”，在登录界面中以 admin.组名.vnn 的帐号登录，即可看到下图：



在上图的界面中，点击“管理”菜单即可看到两个新的选项，一个是“注册新用户”，另一个是“注册网关用户”。

※注意：如果您点击管理后看不到“注册新用户”的连接，请先在左侧的帐号列表中点击 admin.开头的帐号，并使其为橘黄色（如上图），再点击管理按钮即可。

在一般情况下，请点击“注册新用户”的连接以注册一个新的成员帐号。

※注意：如果您不清楚网关用户的具体用途，请不要注册网关帐号。请在我们的技术人员的指导下创建和使用该类帐号。

Chapter 2

第二章 系统设置

在注册新用户的界面（如下图），输入一个需要创建的帐号，其中帐号必须大于 2 位，小于 16 位，必须是由半角英文或数字组成。

基本信息 配 置 组信息 管 理

注册新用户：

帐 号： .demogroup.vnn

密 码：

起始时间： 2009-09-14 和本組设置相同

终止时间： 2009-09-21 和本組设置相同

创 建 返 回

在帐号的起始时间和终止时间设定可以决定该帐号的生效和结束时间。该功能通常可以用于将该帐号提供给在一段时间内出差的用户使用。

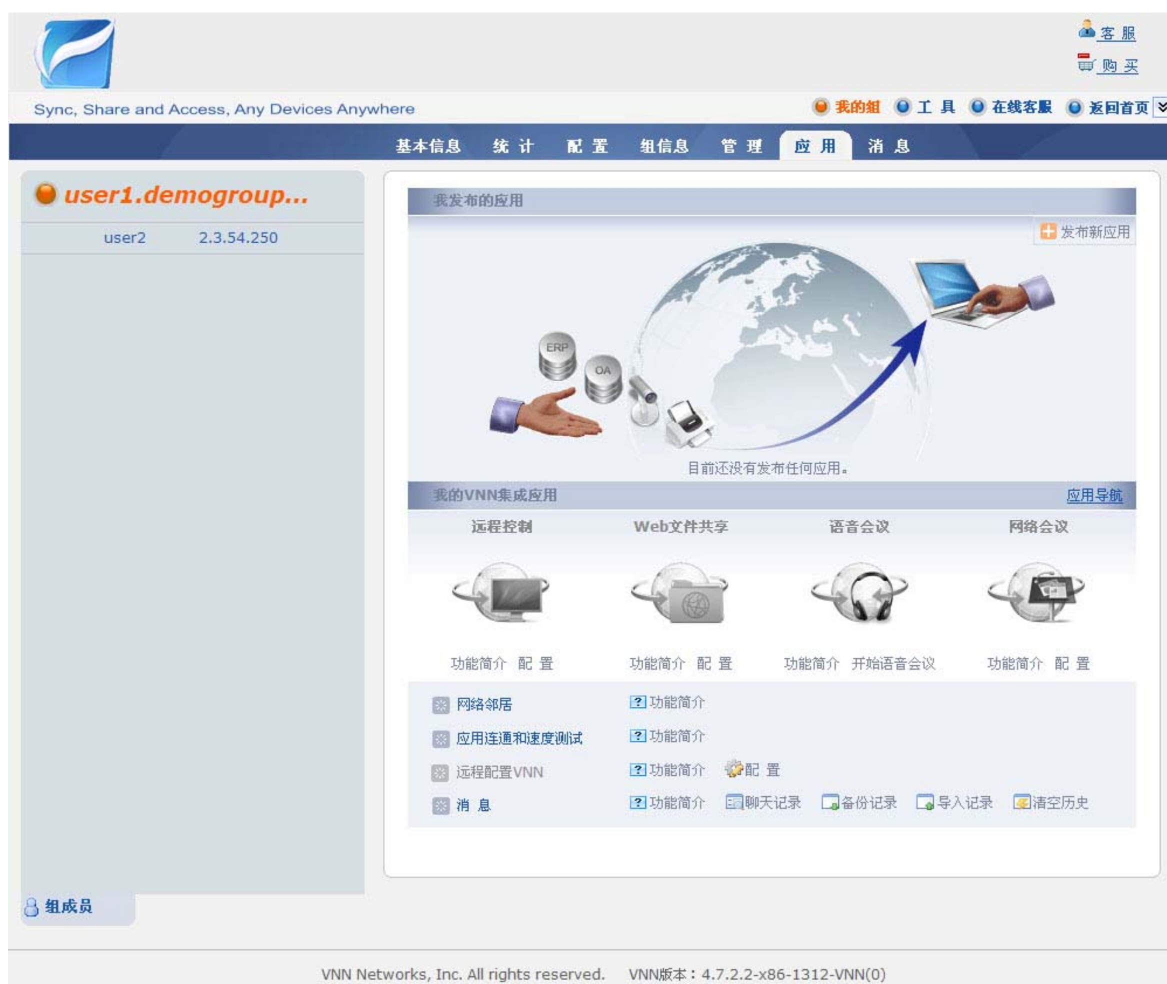
★提示：如果设定了帐号终止时间，在帐号过期后仍然可以通过管理员帐号延长使用时间。

当输入或选择完信息后，点击创建按钮即可创建一个新的成员帐号。

当创建完所需要的帐号后，点击界面右上角的退出连接即可退出管理界面。

2.3 系统>>登录成员帐号

登录一个帐号只需要双击桌面上的“VNN-Enterprise Console”，并在登录中填写需要登录的帐号和密码再点击登录按钮即可。如果帐号和密码正确的话即可出现以下界面：



※ 注意：一台计算机上只能登录一个普通成员帐号或网关帐号，但管理员帐号可以在已登录前任意一种帐号的情况下进行登录。

Chapter 2

2.4 系统>>登录后界面介绍



上图所示的每个标记的解释是：

❶ 当前登录的帐号，帐号被选中时呈现橘黄色，未被选中时呈现蓝色。

❷ 当前组的成员清单，帐号的颜色代表几种不同的状态：

橘黄色：该帐号在线

蓝 色：该帐号目前不在线，但是在 7 2 小时内上过线

灰 色：超过 7 2 小时不在线

❸ 选项卡，通过点击对应的选项卡可以进入针对当前选中的帐号的信息查看或功能设定。

❹ 信息显示或设定界面，通过选定某个帐号或当前已登录的帐号即可查看当前帐号的信息或设定对于当前帐号的信息。

❺ 刷新按钮，用于刷新当前界面的信息。

Chapter 2

2.5 系统>>帐号登出（注销）

如果在一台计算机上退出帐号，那么需要进行注销操作，步骤如下：

双击桌面上的“VNN-Enterprise Console”图标打开 VNN 的登录界面，然后点击“本端当前在线用户”中的帐号，然后填写您的密码并点击登录按钮。如果您选择了“记住输入密码”，那么将会自动进入界面。

当界面载入完成后，点击右上角的“返回首页”右边的下拉箭头（如下图），选择“登出”即可退出当前已经登录的帐号。

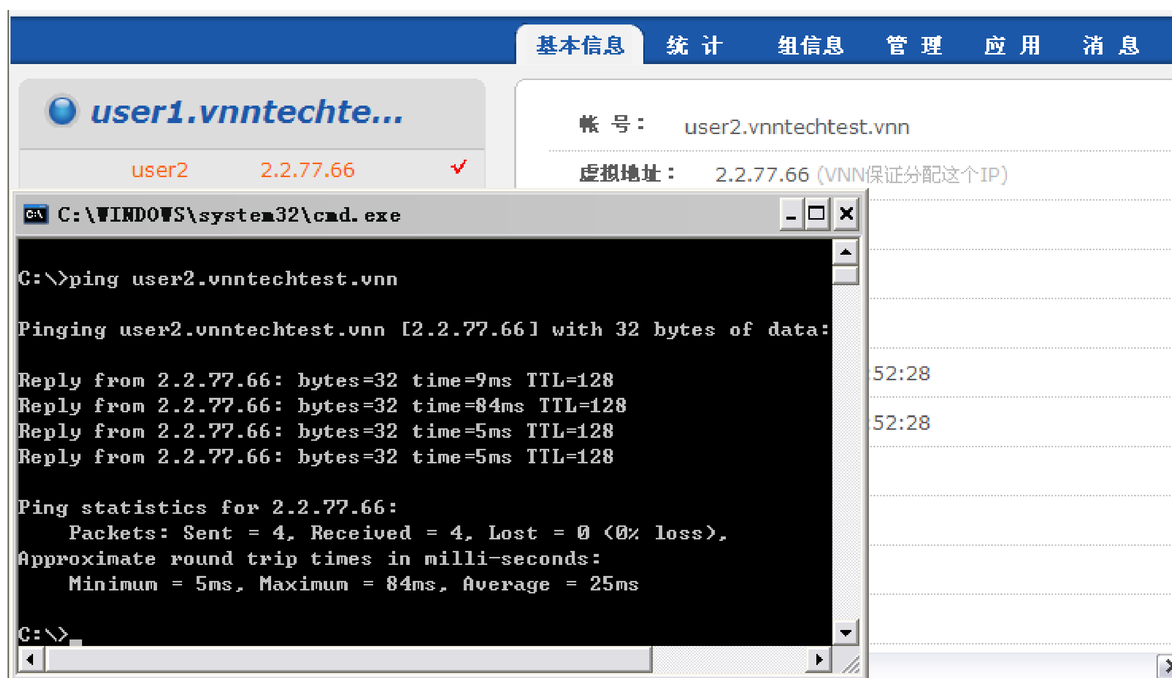


2.6 系统>>测试与对方的连通

在测试开始前，请先确保双方的网络防火墙配置正确，在开始测试前，请先检查双方计算机的网络防火墙配置是否允许 VNN4CSRV.EXE 访问互联网。

点击“开始”菜单，选择运行(或按下 Win+R 键)，输入： ping 对方的 VNN 帐号 。如：ping user2.vnntechtest.vnn ，其中 user2.vnntechtest.vnn 是对方的 VNN 帐号。

如果一切正常，您在界面中看到对方的帐号应该是橘黄色，并且 Ping 的结果应该类似于下图：



※注意：在实际测试中请不要 ping user2.vnntechtest.vnn ，上图中的 VNN 地址仅供本教程演示之用。

2.7 系统>>选项卡功能介绍

在一个成员帐号登录 VNN 后，可以看到以下的选项卡：



其中每个选项卡有着它固定的功能和作用，以下是每个选项卡的功能：

基本信息：用于显示当前或选定的用户的基本信息，包括 VNN 帐号，对应的 VNN 的 IP 地址，编号，起始时间，终止时间，帐号类型，权限，电子邮件和简介。

统计：用于显示所有与本机建立连接的 VNN 帐号信息或显示已选择的帐号的网络信息，包括公网 IP 地址，内网 IP 地址，NAT 类型，心跳包(存活/在线确认包)最后接收和响应时间。

配置：用于配置当前已登录帐号的设置信息。

※注意：对于普通成员帐号，如果在左侧的列表选中的不是自己，那么将看不到配置选项卡。

组信息：显示当前组的组名，组后缀，起始时间，终止时间，组号码，最大用户数，当前用户数，组管理员帐号，邮件的联系地址和简介，是试用还是正式组等信息。

管理：对于普通成员用户，进入该选项卡将提示要求以组管理员登录。如果是管理员帐号，则可以创建组成员用户或网关用户。

应用：检测到对方的的网络通还是不通及通过 Windows 网络邻居访问对方的共享资源。

消息：用于查看其他用户发来的消息或给其他用户发送消息。通过双击列表中的某个帐号可以直接给对方发送消息。

2.7.1 选项卡>基本信息

基本信息 统 计 配 置 组信息 管 理 应 用 消 息

帐 号：	user1.vnntechtest.vnn
虚拟地址：	2.2.77.67 (VNN保证分配这个IP)
编 号：	4000157838
别 名：	
組号码：	29409
起始时间：	2008-10-21 11:52:28
终止时间：	2008-10-28 11:52:28
帐号类型：	普通
帐号权限：	普通用户
我的信任組：	
邮 件：	
简 介：	

2.7.2 选项卡>统计

在选择当前登录的帐号的情况下，点击统计选项卡可以查看哪些 VNN 用户与本机建立了连接，通过单击某一个连接状态可以查看该连接的详细信息(如下图)：

基本信息 统 计 配 置 组信息 管 理 应 用 消 息

UIN	版本	状态	发包	收包	发转包	收转包
4000157837	4040001	在线	86330	56670		

基本信息 在 线 网 络 隧 道

帐 号：

user2.vnntechtest.vnn 虚拟地址：2.2.77.66

最大子网数：0

当前子网数：0

帐号权限：普通用户 帐号类型：普通

起始时间：2008-10-21 11:52:28

终止时间：2008-10-28 11:52:28

简 介：

在上图中出现的浮动信息窗口中可以查看到对方的通信数据和发送 / 接收的数据链路(隧道)，点击不同的按钮可以查看到各种技术信息。

点击红色的 X 即可关闭该浮动窗口。

在基本信息界面中，将显示出对方的基本状态信息

基本信息 在 线 网 络 隧 道

帐 号：

user2.vnntechtest.vnn 虚拟地址：2.2.77.66

最大子网数：0

当前子网数：0

帐号权限：普通用户 帐号类型：普通

起始时间：2008-10-21 11:52:28

终止时间：2008-10-28 11:52:28

简 介：

以下是对于每个项目的解释：

功能名称	解释
帐号	显示对方的帐号名
虚拟地址	显示对方的帐号所对应的 VNN IP 地址
最大子网数	显示对方的网关帐号所能够接受的最大子网数数值（只针对网关帐号）
当前子网数	显示对方的网关帐号当前的子网数数值（只针对网关帐号）
帐号类型	显示对方帐号的权限或类型
帐号权限	显示对方帐号的权限或类型
起始时间	显示对方帐号能够开始使用的时间
终止时间	显示对方帐号的截至到期时间
简介	显示对方帐号的简介（备注）

在线界面中，将能够显示对方的 VNN 版本，在线状态和与对方的流量信息。

基本信息 | 在 线 | 网 络 | 隧 道

核心引擎版本：4040001

在线状态：在线

总共发包：402

总共收包：486

隧道建立：2008-10-27 10:08:17

最后收包：__:__:__

最后发包：__:__:__

收到心跳：2008-10-27 10:08:39

发送心跳：2008-10-27 10:08:39

网速判断：2008-10-27 10:08:24

发送转包：0

收到转包：0

功能名称	解释
核心引擎版本	显示对方的 VNN 的核心引擎版本
在线状态	显示对方是否在线
总共发包	显示从连接上对方开始到现在总共发送了多少数据包
总共收包	显示从连接上对方开始到现在总共接收了多少数据包
隧道建立	显示与对方建立连接开始的时间
最后收包	显示最后从对方计算机收到的数据包的时间
最后发包	显示最后从对方计算机发出的数据包的时间
收到心跳	显示最后收到对方发来的在线确认包时间
发送心跳	显示最后发送给对方的的在线确认包时间
网速判断	显示最后判断与对方之间网络速度的时间
发送转发包	通过本机接收的转发的数据的数据包数量
收到转发包	通过本机发送的转发的数据的数据包数量

基本信息 在 线 网 络 隧 道

公网地址：219.143.151.31北京市 电信

内网地址：10.99.99.111

公网端口：62262 内网端口：42906

增量类型：0 增量数值：0

TTL：未知 NAT类型：Cone

目标地址相关：Yes Plusx值：0

企业专转：No DHCP：Yes

地址池支持：No 校验和支持：No

UPnP：No TCP端口组：0,0,0,0

同端口支持：No 端口映射：No

功能名称	解释
公网地址	显示对方的公网 IP 地址与网络位置
内网地址	显示对方的内网 IP 地址
公网端口	显示对方的 VNN 所使用的公网端口
内网端口	显示对方的 VNN 所使用的内网端口
增量类型	显示对方的网络 NAT 设备的增量类型
增量数值	显示对方的网络 NAT 设备的增量数值
TTL	显示从本机到对方的 TTL 数值
NAT 类型	显示对方的 NAT 网络类型
目标地址相关	显示对方的目标地址相关的是与否
Plusx 值	显示对方的 NAT 设备和网络的 Plusx 值
企业专转	显示对方是否支持企业专用转发功能
DHCP	显示对方是否通过 DHCP 方式获得公网或内网物理 IP 地址。
UPnP	显示对方网络是否支持 UPnP 功能
TCP 端口组	显示对方所使用的 TCP 端口组
同端口支持	显示对方的网络是否支持同端口支持
端口映射	显示对方是否使用了端口映射功能
地址池支持	显示对方的网络是否存在地址池
校验和支持	显示对方的网络是否使用了校验和支持功能

基本信息 在 线 网 络 隧 道

61.132.220.2:668 10.99.99.111:10000
61.132.220.2:668
对端地址：61.132.220.2 对端端口：668
类型：UDP TTL：1
本端地址：10.99.99.48 本端端口：1537
隧道建立：2008-10-27 10:09:53
最后收包：__:__:__
最后发包：__:__:__
收到心跳：2008-10-27 10:10:08
发送心跳：2008-10-27 10:10:40
网速判断：2008-10-27 10:09:53
网速(毫秒)：71
总共发包：440 总共收包：264
发送转包：0 收到转包：0

功能名	解释
对端地址	显示从本机到对端的物理 IP 地址
对端端口	显示从本机到对端的物理 IP 地址所对应的端口
TTL	显示从本机到对方的 TTL 数值
类型	显示建立隧道所使用的 IP 协议类型
本地地址	显示本机建立隧道所使用的 IP 地址
网速	显示从本机到对端建立隧道所用的时间
总共发包	显示从连接上对方开始到现在总共发送了多少数据包
总共收包	显示从连接上对方开始到现在总共接收了多少数据包
隧道建立	显示与对方建立连接开始的时间
最后收包	显示最后从对方计算机收到的数据包的时间
最后发包	显示最后从对方计算机发出的数据包的时间
收到心跳	显示最后收到对方发来的在线确认包时间
发送心跳	先随最后发送给对方的的在线确认包时间
网速判断	显示最后判断与对方之间网络速度的时间
发送转发包	通过本机接收的转发的数据的数据包数量
收到转发包	通过本机发送的转发的数据的数据包数量

2.7.3 选项卡>配置

在该选项卡中，可以修改当前已登录的普通成员帐号的各种信息（如下图）

基本信息 统 计 配 置 组信息 管 理 应 用 消 息

配置用户 user1.vnntechtest.vnn:

☐ 当Windows启动后自动登录本帐号。

☐ 显示被标记为删除的组成员。

☑ 保存消息历史记录

修改密码

密 码：

确 认：

提 交

邮 件：

<输入邮件地址>

提 交

简 介：

<输入简介信息>

提 交

防火墙

单播防火墙

配 置

2.7.3.1 防火墙

※注意：配置 VNN 的网络防火墙需要一定的网络安全知识，如果您不了解有关信息，请不要对防火墙进行配置，否则会导致 VNN 工作不正常。

VNN 内置了防火墙功能。VNN 内置的防火墙用于控制什么应用程序可以使用什么协议或端口在 VNN 的安全隧道里面通讯。如果您的计算机有安装操作系统自带的个人防火墙，可以将 VNN 的网段加入防火墙的例外名单中。

这样，Windows 的个人防火墙将允许任何程序和协议使用 VNN 的隧道。用户可以通过使用 VNN 的防火墙来进一步限制只有某些程序或协议可以通过 VNN 的隧道。为了防止病毒等程序通过 VNN 隧道传播，可以启用 VNN 的防火墙，只允许自己企业的程序使用 VNN 而禁止任何其它的程序使用 VNN 的隧道。这样可以有效地阻止病毒通过 VNN 传播。

如果您对您的操作系统的个人防火墙配置精通的话，可以将 2.0.0.0/255.0.0.0 加入您的个人防火墙的例外区域中(或称为可信区域或白名单)。

配置 VNN 防火墙的方法是：以当前登录的帐号登录 VNN，点击配置选项卡，在配置选项卡界面的最下方是防火墙的配置。

通过下拉列表可以选择希望配置的防火墙类型。单播防火墙指一般的点对点的 UDP 数据包或 TCP 连接，多播防火墙指的是一般的广播数据如 UDP 的广播包。一般情况下，只需要配置单播防火墙的策略。

配置用户 user1.vnntechtest.vnn:

单播防火墙 ○启 用 ⊙禁 用 | 缺省所有包: ⊙允许 ○阻止 所有规则

	应用組	描述	对端帐号	对端端口	本地端口	协议
	core game	war3&sc	所有	所有	6111-6112	TCP
	core game	war3&sc	所有	6111-6112	所有	TCP
	core game	age3	所有	所有	80	TCP
	core game	age3	所有	80	所有	TCP
	core game	age3	所有	所有	2300	TCP
	core game	age3	所有	2300	所有	TCP
	core game	cs	所有	所有	27030-27039	TCP
	core game	cs	所有	27030-27039	所有	TCP
	core media	iTunes	所有	所有	3689	TCP
	core media	iTunes	所有	3689	所有	TCP
	core game	war3&sc	所有	所有	6111-6112	UDP
	core game	war3&sc	所有	6111-6112	所有	UDP
	core game	cs	所有	所有	1200	UDP
	core game	cs	所有	1200	所有	UDP
	core game	cs	所有	所有	27000-27015	UDP
	core game	cs	所有	27000-27015	所有	UDP
	core game	age3	所有	所有	2300-2310	UDP
	core game	age3	所有	2300-2310	所有	UDP
	core media	iTunes	所有	所有	5353	UDP
	core media	iTunes	所有	5353	所有	UDP

只有点击"提交"按钮收到成功的返回时，修改的配置才会被保存生效。

上 移 | 下 移 | 添 加 | 禁 用 | 删 除 | 修 改 | 提 交 | 取 消

上图是 VNN 的防火墙设置界面，VNN 的防火墙是基于数据包过滤的包过滤防火墙，您必须知道您的应用的具体端口或端口范围以及目的地址。

※注意：一般情况下 VNN 的单播防火墙是出于不启用状态，多播防火墙是出于启用状态。您需要进入对应的防火墙并点击“启用”单选框才能够使其生效。

点击添加按钮可以添加一条新的策略并立即生效。通过选中某条策略并点击上移或下移按钮可以调整该策略的优先级。选中一条策略并点击禁用按钮可以使该条策略失效(失效后该条策略左边的生效的绿色图标会变成灰色)。选中一条策略并点击删除按钮可以彻底删除该条策略。选中一条策略并点击修改按钮可以修改该策略。点击返回按钮将返回配置选项卡。

在点击添加按钮后，可以看见如下图所示的界面。在该界面中可以设定。

单播防火墙

应用组	
描述	
协议	UDP
对端帐号	所有
对端端口	1 - 65535 ☑所有
本地端口	1 - 65535 ☑所有
动作	允许

确 定　取 消

在应用组中可以输入该条规则的简单描述，可以是应用程序的名称或其它自定义内容。

在描述中可以输入针对该策略的介绍或其他自定义的内容。

在协议中可以选择 TCP 或 UDP 协议，注意：两者只能选一，如果要同时创建 TCP 和 UDP 的规则，那么需要创建两条策略。

在对端帐号中可以选择该条策略针对所有帐号生效或只某个特定的帐号生效。

在对端端口和本地端口中可以决定策略彼此作用的端口号或端口范围。

在动作中可以选择该条策略的具体行为是允许还是阻止。

下面是一个防火墙示例：

某公司财务部(User1.vnntech.vnn)和销售部(User2.vnntech.vnn)希望通过 VNN 互通基于 SQL Server 的财务数据，但是财务部只希望销售部访问，不希望其它该组的用户访问财务部，同时只希望销售部访问 SQL Server，不希望访问到文件共享。在财务部的 VNN 的防火墙中的具体的配置如下：

进入单播防火墙设置，并点击“启用”，在缺省所有包中选择“阻止”，然后在“所有规则”下拉列表中选择“自定义规则”并点击“添加”按钮。

在应用组中输入“SQL Server”，在描述中输入“财务数据”，协议选择“TCP”，对端帐号选择“User2.vnntechtest.vnn”，取消本端端口中的“所有”复选框，并在复选框中填入 1433－1433 ，对端端口保持默认不变，然后动作选择“允许”，并点击提交按钮（如下图）。

单播防火墙

应用组	SQL Server
描述	允许销售访问数据库
协议	TCP
对端帐号	user2.vnntechtest.vnn
对端端口	1 - 65535 ☑所有
本地端口	1433 - 1433 ☐所有
动作	允许

确 定　取 消

在提交后，规则看起来应该类似于下图：

配置用户 user1.vnntechtest.vnn:

单播防火墙 ⦿启 用 ○禁 用 | 缺省所有包: ⦿允许 ○阻止　自定义规则

	应用组	描述	对端帐号	对端端口	本地端口	协议
✓	SQL Server	允许销售访问...	user2.vnntec...	所有	1433	TCP

以上就完成了操作，该条规则和防火墙的全局设定将只与允许销售部(User2.vnntech.vnn)帐号访问财务部(User1.vnntech.vnn)账号的 1433 端口的 SQL Server 服务，其他该组的任何成员都将无法访问财务部(User1.vnntech.vnn)的任何端口和应用。这样不但控制了什么用户可以访问该服务器，也阻止了可能的病毒的传播。

接上图，当 Windows 启动后自动登录本帐号：该功能用于在 Windows 启动后，并且在登录帐户前自动登录当前登录的帐号。通常用于企业部署或远程管理时使用。普通用户选中此提示可以避免在固定的计算机上重复登录带来的麻烦。

显示标记为已删除的成员：选中此项后，将在组成员列表中显示已经被删除的帐号。如果您希望查看该组中已经被删除的帐号，可以选中此项。
★提示：通常为了保证成员列表的简洁，我们不建议您选中此项。

修改密码：修改当前帐号的密码，输入完毕后点击右边的提交按钮以应用新密码。
邮　　件：用于联系当前帐号所有者的邮件地址，方便其他用户使用。
简　　介：介绍当前帐号的所有者的信息或填写其他内容， 例如该用户的电话等。
防 火 墙：该功能用于控制 VNN 的访问功能，在下拉列表中选择需要配置的防火墙，点击配置按钮即可进行配置。

※注意：通常情况下我们不建议用户修改防火墙配置，否则有可能导致 VNN 工作不正常。如果您有兴趣了解防火墙的详细配置，请参阅 2.3 节的防火墙配置。

2.7.4 选项卡>组信息

基本信息　统 计　配 置　组信息　管 理　应 用　消 息

组 名：	vnntechtest
组后缀：	.vnn
起始时间：	2008-10-21 11:52:28
终止时间：	2008-10-28 11:52:28
组号码：	29409
最大用户数：	9
当前用户数：	3
组管理员：	admin.vnntechtest.vnn
邮 件：	support@vnner.com
简 介：	
正式组：	你使用的是试用組。 已经试用了 0 天，还可以继续试用 6 天。 试用过期后，将不能再登录使用。 要注册成为正式組，请访问官方网站http://www.bizvnn.cn。

2.7.5 选项卡>管理



2.7.6 选项卡>应用 （具体使用方法请参照目录第 9 项）



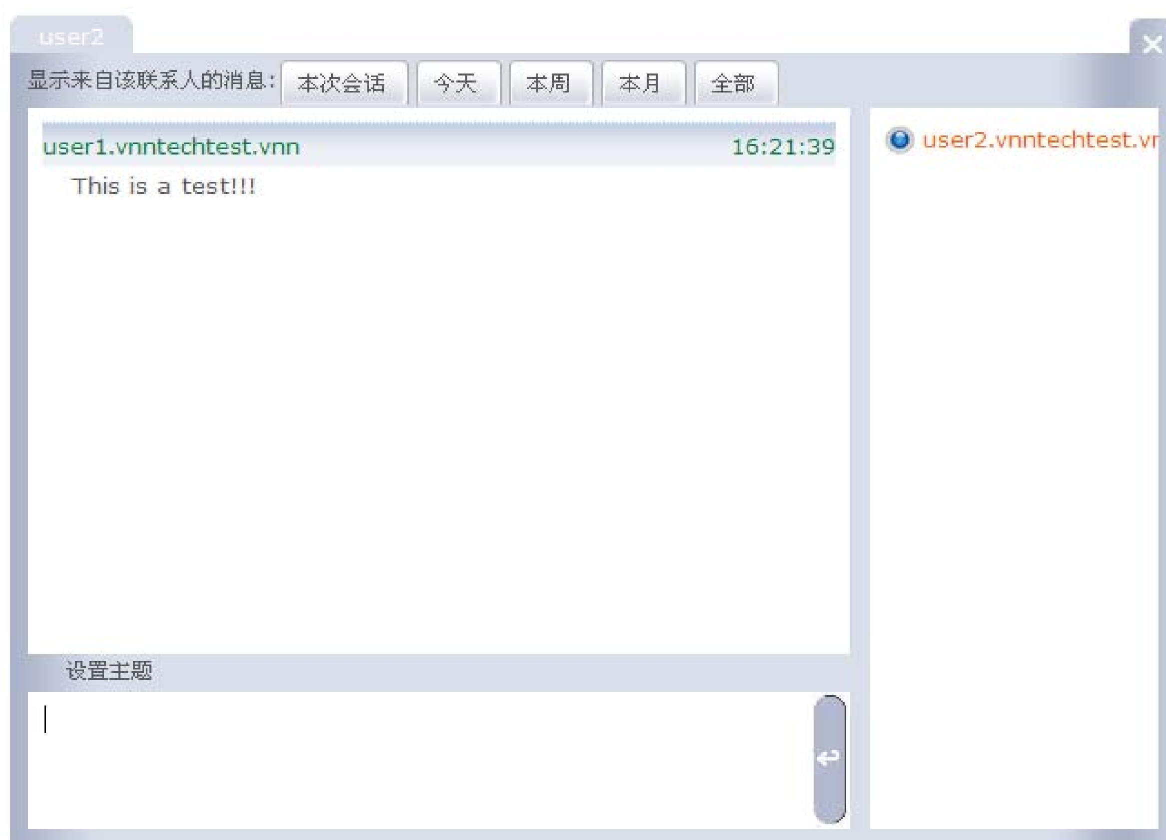
2.7.7 选项卡>消息

Chapter 2

VNN 支持点对点消息发送和多人会议功能，通过右击对方的帐号并选择“发送信息”或者双击对方的帐号即可与对方开始聊天。



如果有新消息来到时，位于操作系统系统栏任务图标区中的 VNN 图标将会显示一个白色的 i ，告知您收到了新的消息。通过右击该图标，选择“启动控制界面”并登陆，即可查看消息。



上图即是聊天时的界面通过点击界面上方的五个按钮可以显示最近或所有的聊天记录，通过点击设置主题按钮，可以为本次的聊天内容设置主题。

在界面的右侧能够显示出当前与您聊天的成员信息，其中橙色显示的为在线，蓝色显示的则为离线。

如果您需要邀请其他人加入对话，可以在界面左侧的用户列表中右击对方的帐号，选择“邀请会话”即可发起新的多人会议并将对方邀请至会议中。

通过指向聊天对话框上方的“消息”选项卡，您还可以查看到之前的聊天记录，备份记录，导入／导出聊天记录，以及清空您所有的聊天记录等与聊天有关的功能。



Chapter 2

2.8 系统>>系统菜单功能介绍

系统菜单中包括“我的组”，“工具”，“退出”三个菜单，“工具”菜单在下文会详细介绍，其中包括“网络信息”，“选项”，“事件”，“备份”，“新功能”，“关于”五个菜单。

2.8.1 系统菜单>我的组



“我的组”菜单只会在帐号登录后出现，点击“我的组”菜单可以从 VNN 的其他操作界面立即切换到当前选中帐号的基本信息选项卡上。

2.8.2 系统菜单>退出



点击“退出”菜单后 VNN 会从当前界面自动返回到登录状态，但是并不会注销 VNN。

2.8.3 系统菜单>工具

2.8.2.1 网络信息

该页面中显示用户当前的内网和公网 IP 地址，以及所处的网络环境信息，包括 NAT 类型等。该类信息用于提供给技术人员相关的诊断信息。点击右侧的绿色向下箭头会显示更多详细信息。

2.8.2.2 选项

在该页面可以设置 VNN4 的事件日志(LOG)级别，当点击“选项”-“日志级别”连接后将会看到如下图的界面：

语言

点击语言下方的下拉框可以选择界面显示语言，目前只有中文和英文选项

日志级别：日志级别功能是提供给 VNN 的技术人员进行错误分析和调试的。如果您在没有我们技术人员的指导下最好不要将该日志级别进行调整。

如果您在使用 VNN 的过程中没有遇到任何错误，可以将日志级别调整到最小日志。

※注意：如果日志级别被调整到最高(最详细日志)，VNN 的传输效率可能会下降。

通过点击选项左边的小 + 号可以看到隐藏的高级设置功能，点击“高级”的连接就可以进入高级选项设置(如下图)。

⊞ 远程配置

⊞ 网关模式 （VNN核心引擎将重启）

⊞ 自定义加密算法

⊞ 核心引擎服务运行身份

⊞ 内置代理设置

※注意：如果您对设置不清楚或不了解，请不要修改这些设置，某些功能是提供给您网络的网络管理员使用的。

远程控制管理：提供中央管理员远程登录此 VNN 账号界面并帮助此 VNN 账号使用者修改其参数设置或者维护其账号，能够让网络管理员远程帮助用户登录或登出 VNN 帐号，进行远程管理。

激活这个选项将允许远程管理你安装在本端上的VNN核心引擎。你必须为这个功能设置一个控制密码！当然你必须记住密码，否则你只能重新安装VNN引擎。当密码设定后，即使在本地进入VNN界面时也需要输入该控制密码（在一台机器上只需要输入一次，然后界面会自动记住），该密码缺省是'admin'，当你启用远程控制时，指定的密码必须不同于缺省密码。

☐ 允许远程控制管理

密 码：

确 认：

保 存

※注意：该功能与操作系统的远程桌面无关。

网关模式：网关模式是一种在本地局域网中更加方便的 VNN 使用方式，该功能能够让当前局域网中只在一台计算机上安装 VNN，其他希望接入 VNN 网络的计算机不需要安装 VNN 客户端软件，只需要配置一个到该计算机的 VPN 连接即可。在稍后的章节中我们将详细介绍该功能。

当需要使用VNN网关帐号时，你需要勾选下面的选项。VNN网关能让同一局域网内的其它机器无需安装VNN客户端也能连入VNN虚拟网络。这样，非windows系统的机器也就可以使用VNN的安全虚拟局域网功能了。如何配置不同操作系统的使用VNN请访问我们的官方网站 http://www.bizvnn.cn。

☑ 网关模式运行

自定义加密算法：该功能决定了 VNN 使用哪种加密算法与其他 VNN4 发送数据，其中：

◉ RC4
○ AES(128位)
○ AES(256位)

保 存

RC4：(Rivest 密码法 4)是使用最广泛的软件流密码和被用在通俗协议例如安全套接字层 (SSL)（来保护因特网传输）和 WEP（来保护无线网络）。RC4 产生位的一个伪随机流（一个“密钥流”）；解密以相同的方式执行。

AES：(高级加密标准)是一个用来代替数据加密标准（DES）的算法。目前使用的一般为 128 和 256 位密钥，这三种密钥位数代表不同的安全级别，位数越高安全性越高。选择任何一种加密算法都能够被信息传递的目标方的 VNN 正确的解开，用户可以任选其一。

核心引擎服务运行身份：

VNN 核心引擎服务所运行的帐号身份缺省使用的是 Windows 内置的“LocalSystem”身份。由于“localsystem”是没有访问网络资源权限的帐号。所以在某些场合下，比如需要使用网络共享时，请切换到有权限使用网络资源的身份帐号，比如"Administrator"。

您可以改变VNN核心引擎服务所运行的帐号身份，缺省使用的是Windows内置的"LocalSystem"身份。在某些场合，比如需要使用网络共享时，请切换到有权限使用网络资源的身份帐号，比如"Administrator"。

用户名： LocalSystem ☑ 缺省身份

密 码：

☐ 域 名：

提 交

内置代理设置：

VNN 内置了 SOCKS5 代理服务器，当你需要使用代理服务器时，可以直接使用，而无需额外安装其它的代理服务器。

VNN内置了SOCKS5代理服务器，当你需要使用代理服务器时，可以直接使用，而无需额外安装其它的代理服务器。

本地VNN端口： 2387

状态： 启 用

通过点击选项左边的小 + 号可以看到隐藏的网络设置功能，点击“网络”的连接就可以进入网络选项设置(如下图)。

VNN使用UDP封装以穿透NAT设备，通常情况下，只要您能正常访问网站，就能正常使用。如果您无法登录或者速度很慢，请允许到这台VNN机器的所有UDP，或者如果您的防火墙策略无法允许所有的UDP通过，请根据您的网络环境激活下列的配置之一。如果仍然无法解决，请联系我们的技术支持。

⊞ **我的防火墙阻止了部分UDP，配置VNN能使用的UDP端口**

⊞ **我的防火墙只允许VNN使用一个UDP端口，配置VNN使用这个被映射的端口**

⊞ **我的防火墙只允许VNN使用一个UDP端口，且无法配置映射**

⊞ **我的网络非常特殊，配置VNN使用TCP转发所有数据**

我的防火墙阻止了部分 UDP，配置 VNN 能使用的 UDP 端口：

VNN使用到UDP，如果您的网络安全策略无法支持将防火墙配置成允许到这台安装了VNN的机器的所有进出UDP，那么您至少也需要能允许从这台机器的至少11个UDP端口（即本地端口）发出去的所有包，相应公网返回到这些本地端口的所有UDP包也必须允许。

如果您希望进一步限制允许本地端口发出去的UDP包的目的端口范围，那么请参照缺省目的端口范围那样必须包含668在内的一大段范围（这个目的端口范围同时也是防火墙允许从公网进来的UDP包的源端口范围）。

请您首先在防火墙上配置完成相应的UDP访问规则后，再在下面结合您具体的端口配置细节进行更改。如果您允许了进出本地的所有UDP包，那么您保留下面的缺省值即可。

强烈建议：目的端口使用缺省值以获取最快的连接速度，如果无法做到，请尝试"我的防火墙允许使用一个UDP端口"的配置。

本地端口从

666 -- 49152 ☐ (使用缺省值)

目的端口从

666 -- 57344 ☑ (使用缺省值)

保 存

我的防火墙只允许 VNN 使用一个 UDP 端口，配置 VNN 使用这个被映射的端口：

当您无法配置防火墙允许VNN所需的UDP端口时，可以在接入到公网前的NAT设备上映射一个UDP端口（公网端口），这个端口映射到安装了VNN的机器的IP的某个UDP端口（内网端口），两个端口可以相同，也可以不同；然后只需要配置防火墙允许这一个UDP端口，就能够正常使用了。

对于安全要求比较高的公司，通过这种方式能够让防火墙仅仅需要打开唯一的额外UDP端口。这个映射并不需要有静态公网地址，需要注意的是，如果经过多层NAT接入公网，需要在每个NAT设备上都做映射。

如果您实际网络环境中设备不支持做这个映射，同时又不允许防火墙打开必须UDP端口，请选用"我的防火墙只允许访问网页"的设置。

☐ 使用映射端口

内网端口 0

公网端口 0

保 存

我的防火墙只允许 VNN 使用一个 UDP 端口，且无法配置映射：

当您无法配置防火墙达到上面的要求之一时，VNN不得不通过公网上的UDP 53或668服务器帮您进行通讯，这时，您需要配置防火墙允许本地的UDP 669端口可以与公网的UDP 53或668进行通讯。

注意：这样经过UDP隧道转发的速度会比通过UDP隧道的直连慢很多。

我的网络非常特殊，配置 VNN 使用 TCP 转发所有数据：

当您所处的网络环境无法任意收发UDP包时（通常是防火墙不允许所有UDP通过，并且您无法重新配置防火墙以允许VNN所需的UDP），您可以设置允许VNN通过TCP隧道来转发所有包，那样就也可以上线并且和其他人正常通讯，不过速度会比通过UDP隧道的直连慢很多。

注意：这种情形是指您现在只能浏览网站（也就是说允许TCP 80和443），如果您无法浏览网站，本选项也无法帮助您，请确认您现在的确可以上网。

☐通过TCP隧道转发所有数据

保 存

该功能用于当用户当前的网络封锁了 UDP 协议时，使用 TCP 协议通过服务器转发使用 VNN 的解决方案，如果用户所处的网络没有封锁 UDP 协议，不建议选中此选项。

※注意：启动该功能可能会导致 VNN 的传输速度极大下降

备份：

备份本机帐号和其他 VNN 帐号的聊天记录，注意聊天纪录是保存在本机的系统盘下，一旦格式化系统盘聊天记录就会丢失。

2.8.2.3 事件

该功能提供最近 VNN 的有关事件，包括可能遇到的网络问题，连接问题，登录和注销事件等等。进入该页面后通过点击橘黄色的“详细日志”连接可以下载到提供给 VNN 技术人员的详细分析日志。

★提示：日志会自动删除，通常情况下 VNN 的日志保存在“C:\Program Files\Common Files\VNNShared\VHttpdRoot\LOG\”中（不包含引号），您可以随时手动删除这些日志文件。

2.8.2.4 新功能

介绍当前版本或未来版本的 VNN 所推出的新功能，您可以通过该页面中了解具体的信息。

2.8.2.5 关于

显示 VNN 的版权信息。

Chapter 3

中央集权管理

VNN 集成了中央集权管理功能，每个组的 admin 管理帐号可以对组内成员帐号进行添加，删除，登录计算机 MAC 绑定、防火墙、访问控制列表、个人信息以及网关帐号所特有的子网帐号用户数控制等操作。

客 服
购 买
Sync, Share and Access, Any Devices Anywhere
我的组 工 具 在线客服 返回首页
基本信息 配 置 组信息 管 理

admin.demogroup...
user1 2.3.54.249
user2 2.3.54.250

帐 号： admin.demogroup.vnn 刷 新
虚拟地址： 0.0.0.0
编 号： 4000236668
组号码： 54210
起始时间： 2009-09-14 15:10:45
终止时间： 2009-09-21 15:10:45
帐号类型： 普通
帐号权限： 管理员
我的信任组：
信任策略： 本组和信任组里的成员都可以访问（缺省）
邮 件： admin@vnner.com
简 介： Language:CN;QQ:78992710;Use:1

组成员

 VNN版本：4.7.2.2-x86-1312-VNN(0)

3.1 帐号基本配置

点击左侧的帐号列表中的帐号后，选择配置选项卡，可以看到下图所示。管理员可以更改用户的密码，使用时间，别名，DNS（请单击右侧的问号图标获得使用提示）删除用户等操作。

配置用户 user2.demogroup.vnn: 基本配置

☑ 该成员可以配置个人信息

更改别名

别 名： 提 交

更改DNS

2.3.54.250： 提 交

修改密码

密 码： 提 交

确 认：

邮 件：

<输入邮件地址> 提 交

简 介：

<输入简介信息> 提 交

起始时间：

2009-09-14 ☑ 和本组设置相同 提 交

终止时间：

2009-09-21 ☑ 和本组设置相同

删除该用户

该功能表示该用户将不能正常使用VNN,但是此ID将被长期保留，不能被恢复。（如果您是试用組，则无法使用此功能。） 删 除

★提示：当使用组的管理员帐号登录界面后，在左侧的用户列表中可以看到组内的所有成员清单，其中呈现蓝色的帐号意味着该帐号在 72 小时内登录过，如果某个帐号呈现为深灰色，则意味着该帐号在 72 小时内未登录过。如果是浅灰色，则意味着该帐号已经被删除。

3.2 帐号高级配置

当选中需要被管理的帐号后，在右侧的基本信息列表中将会显示出该帐号的具体信息，通过点击“配置”选项卡，然后从右上角的“基本配置”选项卡中选择“高级配置”即可对该帐号进行管理。

★技巧：通过右击某个帐号即可对该帐号的基本配置和高级配置进行修改。



上图是选中 user2.vnnrtechtest.vnn 帐号，并进入高级配置的界面，在该界面的上方用橙色的字体标注了您当前正在配置的帐号名称。

在该界面中，可以对该帐号的登录控制（MAC 地址绑定），访问控制列表（黑白名单和好友名单），防火墙以及个人信息进行设定。以下是每个功能的介绍：

帐号和 MAC 地址绑定：该功能用于将 VNN 的登录帐号同机器的 MAC 地址绑定，只有当机器的 MAC 地址与 VNN 数据库中所绑定的 MAC 地址匹配时 VNN 才会允许这台机器登录并接入组内网络。一旦 MAC 地址不匹配或更换了计算机，那么该帐号将无法登陆。

通过点击“设置绑定”按钮即可列出该帐号最后一次登录时所使用的 MAC 地址。

通过点击“绑定”连接即可将设定中的帐号与显示的 MAC 地址相互绑定。如果需要解除绑定，那么可以返回该设置，点击“取消绑定”后即可解除绑定。

※注意：MAC 地址绑定某个帐号前，该帐号必须在需要绑定的计算机上登录过一次。如果这个帐号从来没有登录过，是无法进行 MAC 地址绑定的。

Chapter 3

权限管理：

访问控制设置：

本组和信任组里的成员都可以访问（缺省）

配置用户 user2.demogroup.vnn:

访问控制设置

VNN提供了基于用户帐号的访问控制，通过访问策略实现。

请为此用户选择如下访问策略之一：

- (●) 本组和信任组里的成员都可以访问（缺省）
- ( ) 只允许本组成员访问，不允许信任组成员访问
- ( ) 只允许信任组成员访问，不允许本组成员访问

提 交

该选项意味着默认本组的所有成员都可以访问我，和我的的组建立了信任关系的成员也都可以访问我（信任组关系的建立需要 VNN 技术支持人员开通）

只允许本组成员访问，不允许信任组成员访问

配置用户 user2.demogroup.vnn:

访问控制设置

VNN提供了基于用户帐号的访问控制，通过访问策略实现。

请为此用户选择如下访问策略之一：

- ( ) 本组和信任组里的成员都可以访问（缺省）
- (●) 只允许本组成员访问，不允许信任组成员访问
- ( ) 只允许信任组成员访问，不允许本组成员访问

提 交

该选项意味着默认本组的所有成员都可以访问我，和我的的组建立了信任关系的成员也不可以访问我（信任组关系的建立需要 VNN 技术支持人员开通）

只允许信任组成员访问，不允许本组成员访问

配置用户 user2.demogroup.vnn:

访问控制设置

VNN提供了基于用户帐号的访问控制，通过访问策略实现。

请为此用户选择如下访问策略之一：

- ○ 本組和信任組里的成员都可以访问（缺省）
- ○ 只允许本組成员访问，不允许信任組成员访问
- ◉ 只允许信任組成员访问，不允许本組成员访问

提 交

该选项意味着默认本组的所有成员都不可以访问我，和我的的组建立了信任关系的成员可以访问我（信任组关系的建立需要 VNN 技术支持人员开通）

设置完毕后点击提交

配置用户 user2.demogroup.vnn:

访问控制设置

VNN提供了基于用户帐号的访问控制，通过访问策略实现。

请为此用户选择如下访问策略之一：

- ○ 本組和信任組里的成员都可以访问（缺省）
- ○ 只允许本組成员访问，不允许信任組成员访问
- ◉ 只允许信任組成员访问，不允许本組成员访问

提 交

配置防火墙：该功能用于远程指定该帐号的 VNN 防火墙的访问配置策略，在某些情况下用户可能只希望远程客户端访问本机的某一个端口。

配置用户 user2.demogroup.vnn:

单播防火墙 启 用 禁 用 | 缺省所有包：允许 阻止 自定义规则

应用组	描述	对端帐号	对端端口	本地端口	协议

只有点击"提交"按钮收到成功的返回时，修改的配置才会被保存生效。

刷 新 上 移 下 移 添 加 禁 用 删 除 修 改 提 交
应用到全组 从全组删除

应用到全组按钮可以把所添加的策略应用到组内的每一帐号。

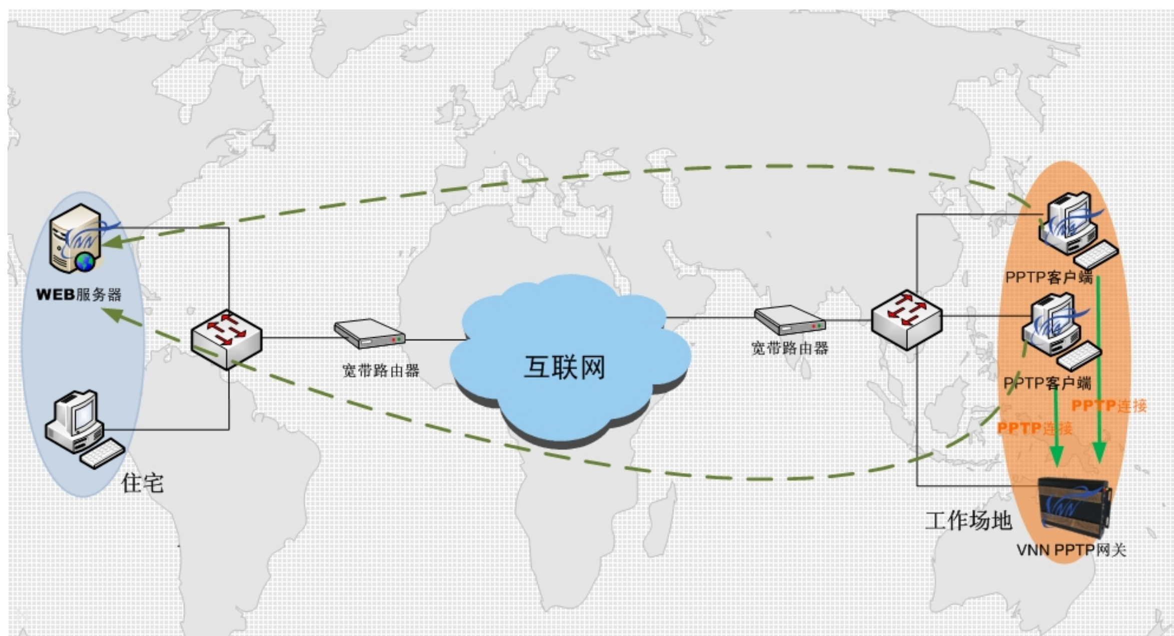
具体的配置，和本手册中的“2.7.3.1 防火墙”章节相同。

Chapter 4

PPTP 网关模式与客户端部署

VNN 支持网关模式，网关模式是一种在本地局域网中更加方便的 VNN 使用方式，该功能能够让当前局域网中只在一台计算机上安装 VNN，其他希望接入 VNN 的计算机不需要安装 VNN，只需要配置一个到该计算机的 VPN 连接即可。

对于企业内部不允许接入互联网的计算机可以通过 PPTP 程序拨号到 PPTP 网关服务器，以下图为例：工作场地内的两台不允许接入到互联网的计算机想要访问住宅中的 WEB 服务器，这两台计算机通过系统自带的 PPTP 程序拨号到局域网中的 VNN PPTP 网关以进入 VNN 的虚拟网络，这样就可以访问登录了 VNN 帐号的住宅内的 WEB 服务器。



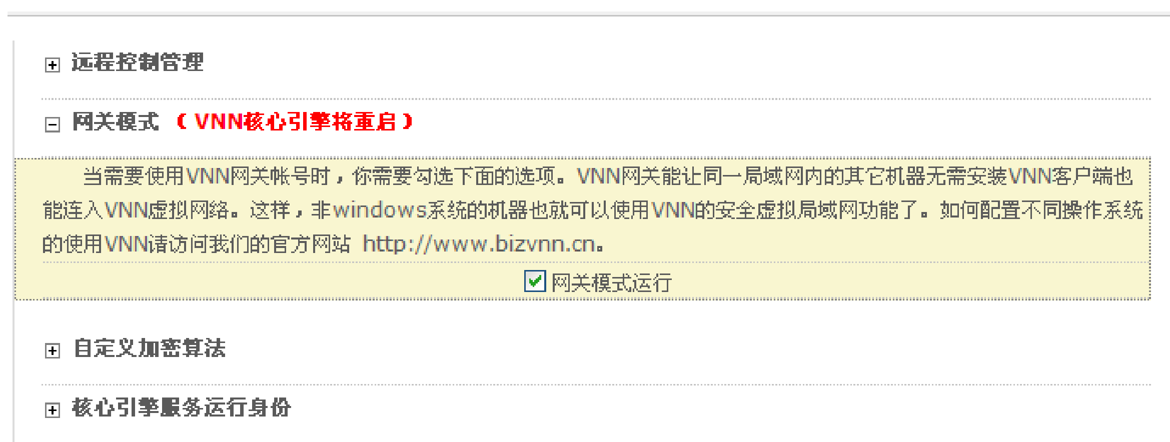
Chapter 4

在开始前，首先需要以组管理员帐号的权限创建一个网关帐号并建立子网用户，同时还需要在局域网中的一台计算机上安装 VNN 并开启网关模式，具体的操作是：

双击桌面上的“VNN-Enterprise Console”，在界面载入完毕后点击右上角的“帮助”，点击左侧树目录中的“选项”左边的 + 号，然后在展开的项目中点击“高级”。（如下图）



然后再右边出现的高级选项中找到“网关模式”项目并点击左侧的 + 号，然后选中“以网关模式运行”复选框。即刻会出现一个新的对话框，提示 VNN 核心引擎正在重新启动，该过程大概需要 2 5 秒。



使用管理员帐号登录后点击配置选项卡按照下图设置：



点击管理选项卡，点击“注册新网关”连接，此时就进入了创建新网关帐号的页面（如下图）。

基本信息　配 置　组信息　管 理　应 用

帐 号：gateway .vnntechtest.vnn
密 码：●●●●●●●
网关容量：3
起始时间：2008-10-21 ☑和本組设置相同
终止时间：2008-10-28 ☑和本組设置相同

创 建　返 回

在帐号处填写需要注册的帐号，在密码中填写为该帐号设定的密码，网关容量填写该局域网中需要接入 VNN 网络的计算机的台数，起始时间和终止时间填写该帐号的有效日期范围或保持默认设置。

设置完毕后，点击创建按钮即可创建该帐号。

※注意：VNN 的网关帐号的网关容量是有限扩容的，能够扩容的数量是当前注册时填写的网关容量的 2 倍。如果创建一个 3 用户容量的的网关帐号，那么在未来该网关帐号就只能扩容到 6 个用户的容量。如果届时需要多于 6 个子网用户，那么必须删除该网关帐号并重建或建立第二个网关帐号。

帐号创建成功后，可以在左侧的帐号列表中找到刚创建的帐号，同时，该帐号的右边会有一个红色的 G 标识，该标志表示该帐号是一个网关帐号。

当网关帐号创建成功后，需要登录该网关帐号并设定该网关中下属的计算机的帐号和密码信息。该操作必须在准备运行 VNN 网关的计算机上进行。

Chapter 4

首先，双击桌面上的“VNN-Enterprise Console”，打开控制界面，在登录处输入刚创建的帐号和密码并登陆，稍后会看到如下的界面：

gateway.demogro...
1 2.3.57.103
2 2.3.57.104
3 2.3.57.105
组成员 子 网

帐 号： gateway.demogroup.vnn 刷 新
虚拟地址： 2.3.57.102 (VNN保证分配这个IP)
编 号： 4000237525
别 名：
域 名：
组号码： 54210
起始时间： 2009-09-14 15:10:45
终止时间： 2009-09-21 15:10:45
帐号类型： 网关
最大子网数： 6
当前子网数： 3
帐号权限： 普通用户
我的信任组：
信任策略： 本组和信任组里的成员都可以访问（缺省）
邮 件：
简 介：

您可以注意到，原先显示组成员帐号的列表变成了 IP 地址，在上图中的 3 个 IP 地址就是在示例中创建的网关的客户端的 IP 地址。目前，这些 IP 地址都没有被分配帐号和密码。

通过选中某个 IP 地址并点击配置选项卡可以为该 IP 地址分配帐号，具体的操作是：
选中左侧列表中的某个 IP 地址，点击配置选项卡，即可看到三个文本框，在帐号中填写希望为该 IP 分配的帐号，在密码中填写希望为该 IP 分配的密码，在别名中可以输入对于该 IP 地址的备注信息(如下图)

帐 号： web
密 码： ●●●●●●
别 名： 用于网关登录
加入批提交队列

当确认无误后，点击“加入批量递交队列按钮”，那么这些信息已经被临时的记录了下来(但是还没有应用生效)。

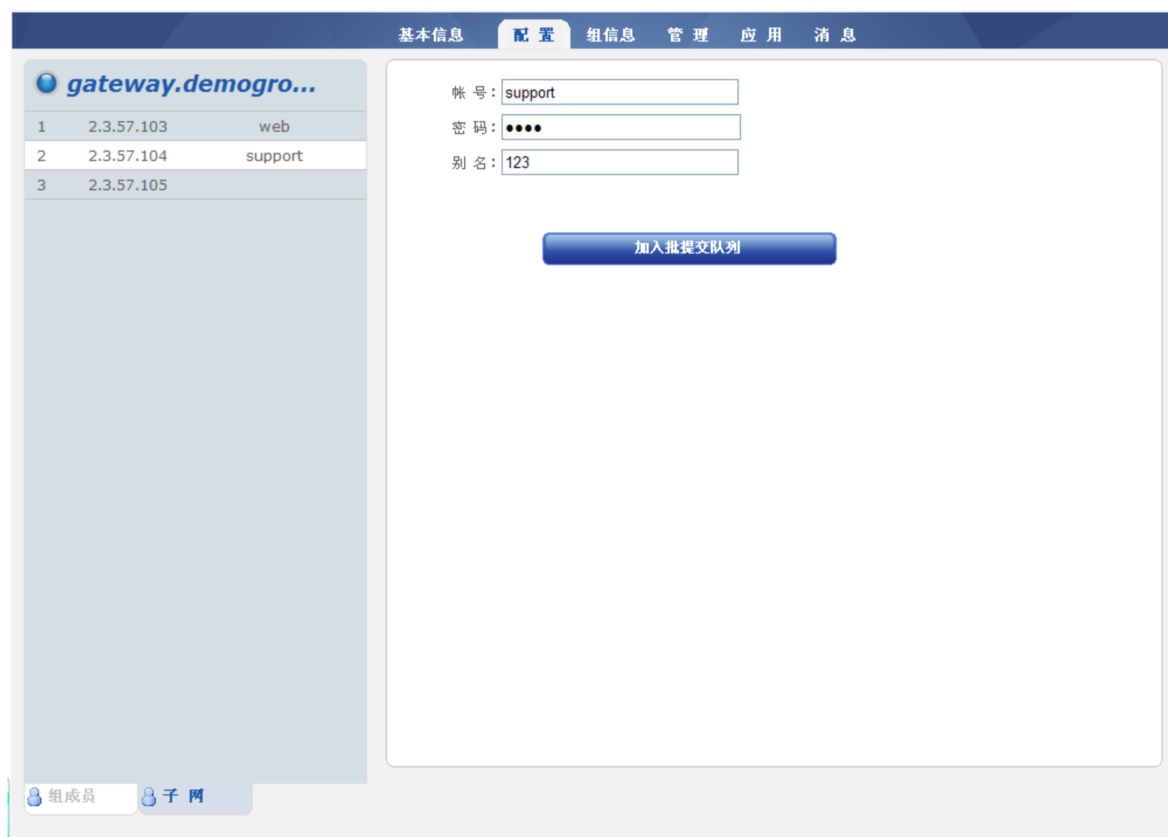
此时，如果您需要在为其他 IP 地址设定帐号和密码，可以重复上一步骤的操作。

当您为所需要的 IP 地址分配完帐号和密码后，请注意界面的底部，会有一个批量提交队列的提示，如下图：



只有当您点击“提交”按钮后，刚才的配置才会生效。

当您点击提交后，左侧的列表的 IP 地址右边会显示出该 IP 地址所对应的帐号，您可以逐一核对该帐号所对应的 IP 地址是否正确。



Chapter

4

以上就完成了在 VNN 网关上的所有配置，下面将在客户端上配置无客户端登录的拨号连接。

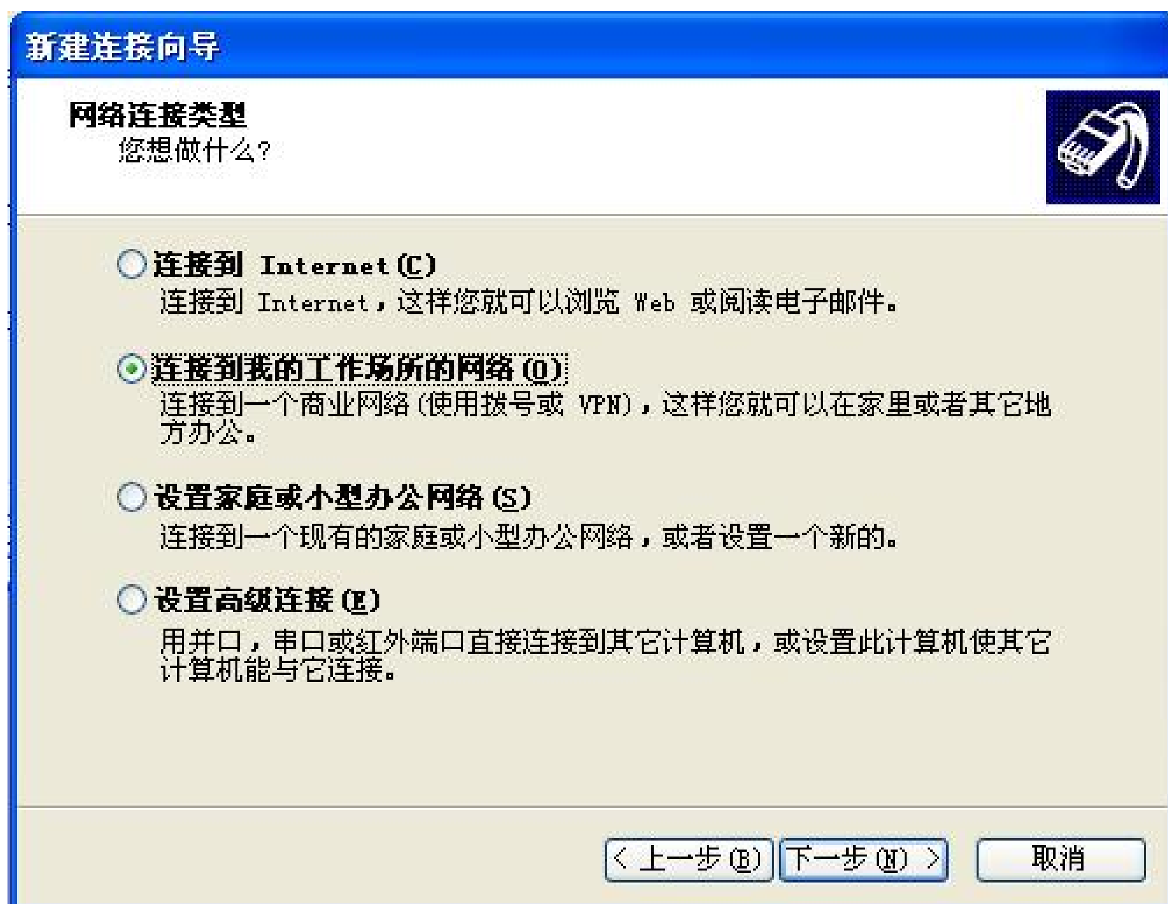
★提示：VNN 网关计算机上最好不要有网络防火墙，否则会导致 VNN 的连接不正常。

※注意：以下教程基于 Windows XP SP2 进行，理论上 VNN 网关支持所有支持 PPTP VPN 拨号的连接。

点击“开始”菜单，选择“控制面板”(某些计算机可能是设置->控制面板)，然后进入“网络和 Internet 连接”，然后进入“网络连接”(某些计算机可能可以直接看到“网络连接”图标)，然后点击左侧的“创建一个新的连接”连接(某些计算机可能可以看到“创建新连接”图标)。
操作系统将会启动一个“新建连接向导”向导，点击“下一步”按钮继续。



在第二步中，向导会询问您的网络连接类型，选择“连接到我的工作场所的网络”，并点击下一步按钮。



在第三步中，向导会询问您以何种类型进行连接，选择“虚拟专用网络连接”，并点击下一步按钮。



在第四步中，向导会询问您的公司名称，在该文本框中您可以输入任何内容。输入完毕后请点击下一步按钮。

在第五步中，向导会询问您 VPN 服务器的名称或地址是什么，请输入您本地网络中的 VNN 的网关服务器的物理 IP 地址。也就是之前本教程所提到的，启动了网关模式，登陆网关帐号并且为 IP 地址分配了帐号的计算机的物理 IP 地址。当填写完毕后，请点击下一步按钮继续。

新建连接向导

VPN 服务器选择

VPN 服务器的名称或地址是什么?

输入您正连接的计算机的主机名或 IP 地址。

主机名或 IP 地址(例如，microsoft.com 或 157.54.0.1)(H):

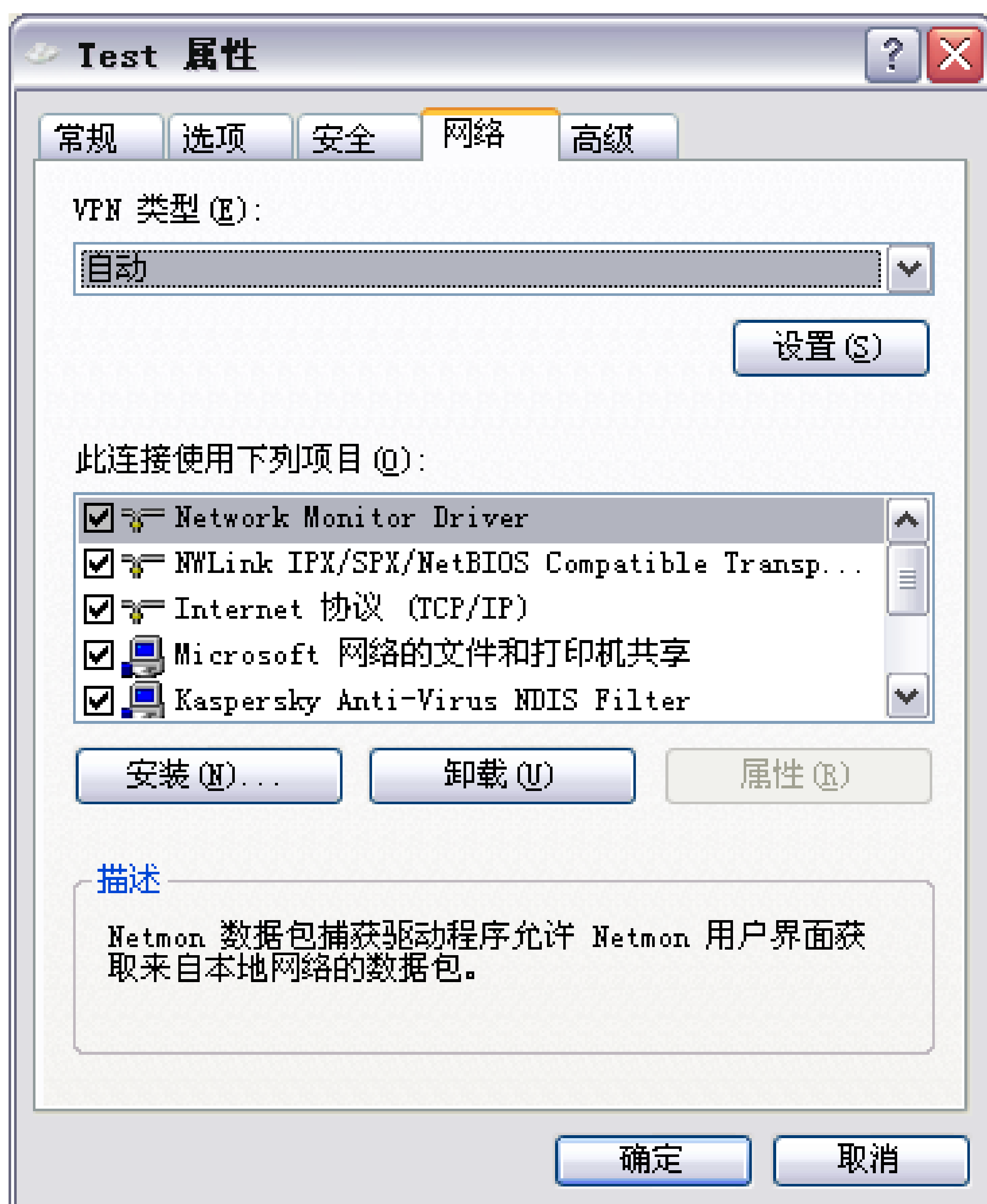
192.168.100.110

< 上一步(B)　下一步(N) >　取消

在第六步，向导提示创建成功，请点击完成按钮完成该向导。

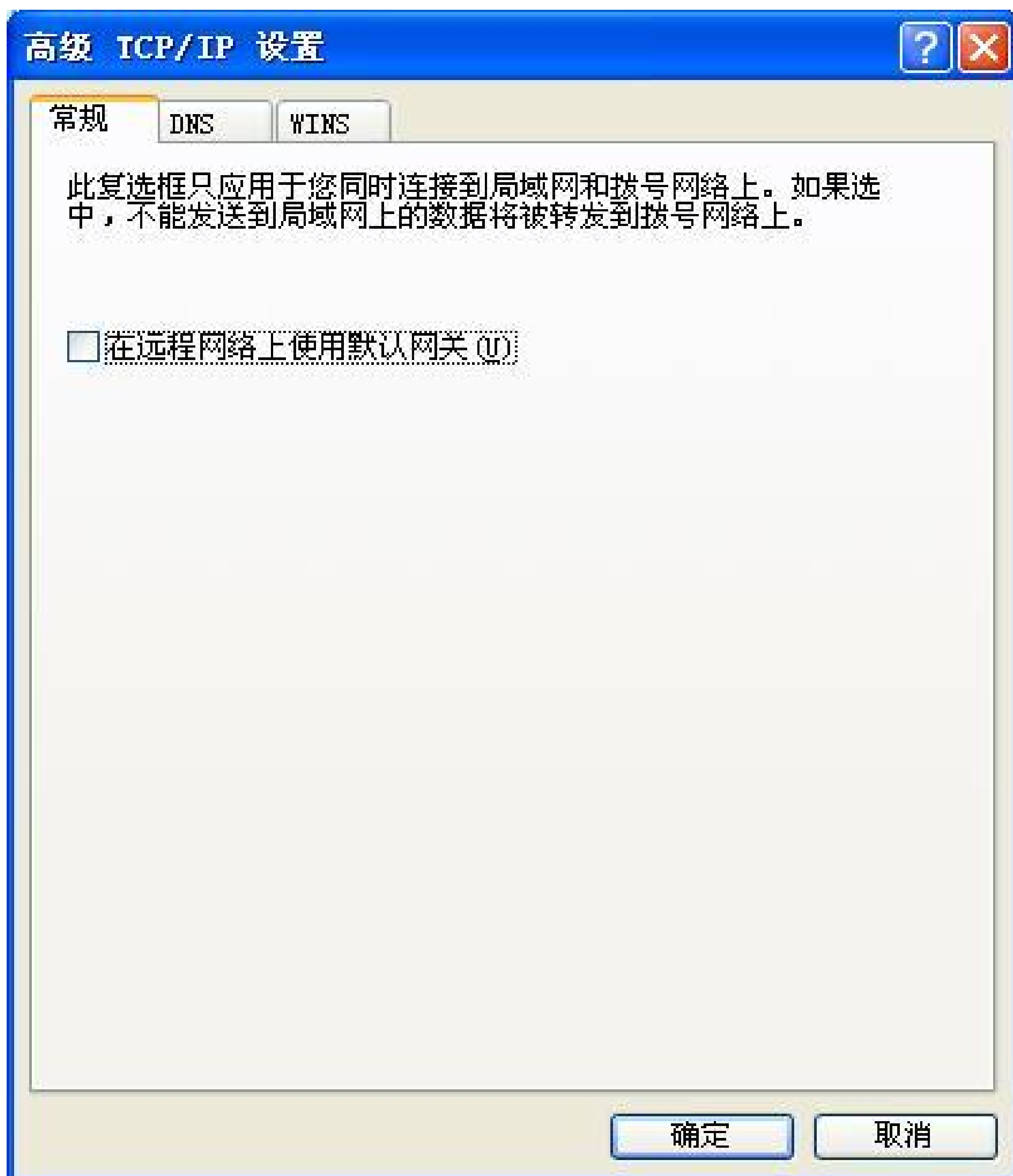
然后，在网络连接对话框中会多出一个您刚才创建的连接，我们还需要调整一下该连接以免造成您的物理网络访问异常。

★提示：创建成功后操作系统可能会自动打开该连接并提示您输入帐号密码，请先点击取消或关闭按钮继续配置。



右击刚才创建的连接，选择属性。在出现的属性对话框中点击“网络”选项卡，然后找到并选中“Internet 协议(TCP/IP)”，并点击属性按钮。

然后，在新出现的窗口中点击“高级”按钮，即可在常规选项卡中看到一个名为“在远程网络上使用默认网关”的复选框，取消该复选框，并点击确定按钮直。至此就完成了该连接的配置。



下面，请双击该连接，在连接中要求输入帐号和密码的地方按照以下格式填写：
帐号格式为： 在网关上创建的帐号.网关帐号

举例说明：比如您的网关帐号是 gateway.vnntechtest.vnn ，您在网关帐号上创建的客户端的帐号是 web ，那么在此处需要输入 web.gateway.vnntechtest.vnn 。

密码为您在网关上为改帐号分配的密码，类似于下图：



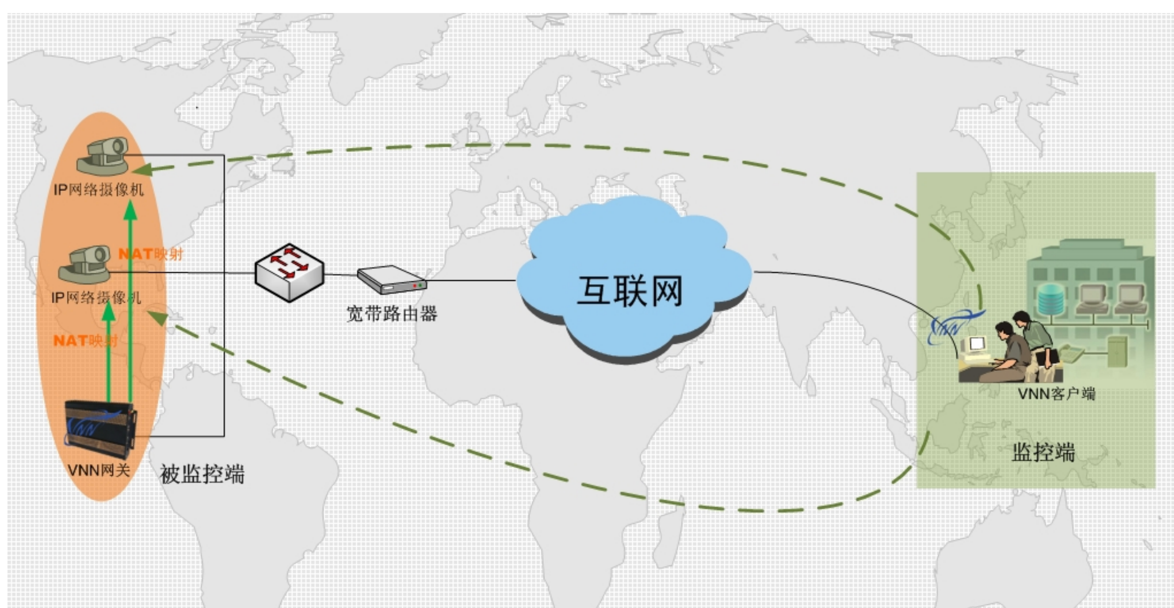
当您点击连接按钮，如果一切配置正确，您应该会立即在任务栏右下角的图标区看到“现在已连接”的提示。

Chapter

5

NAT 网关模式安装与配置

VNN 的 NAT 网关模式是用于远程访问某些局域网里面的服务器，并且该服务器不能安装 VNN 的客户端软件。通过使用 VNN 的 NAT 网关模式， 可以映射 VNN 的 IP 到该服务器的内网 IP，从而实现远程安全访问。



Chapter 5

VNN 支持 NAT 网关功能，能够给本地网络中无法安装 VNN 的网络设备或非 Windows 操作系统主机如 Unix,Linux,Mac,Sybian 等系统，网络打印机，网络摄像头等提供通过 VNN 远程访问的功能。

在使用该功能前，您必须准备一个网关帐号，而网关帐号的子网容量则决定您需要映射的设备数量。比如您只有一个网络打印机需要远程访问，那么您的网关帐号就只需要一个子网帐号。

关于网关帐号的创建方法，请参阅第四章节的《PPTP网关模式的使用与客户端的部署》。

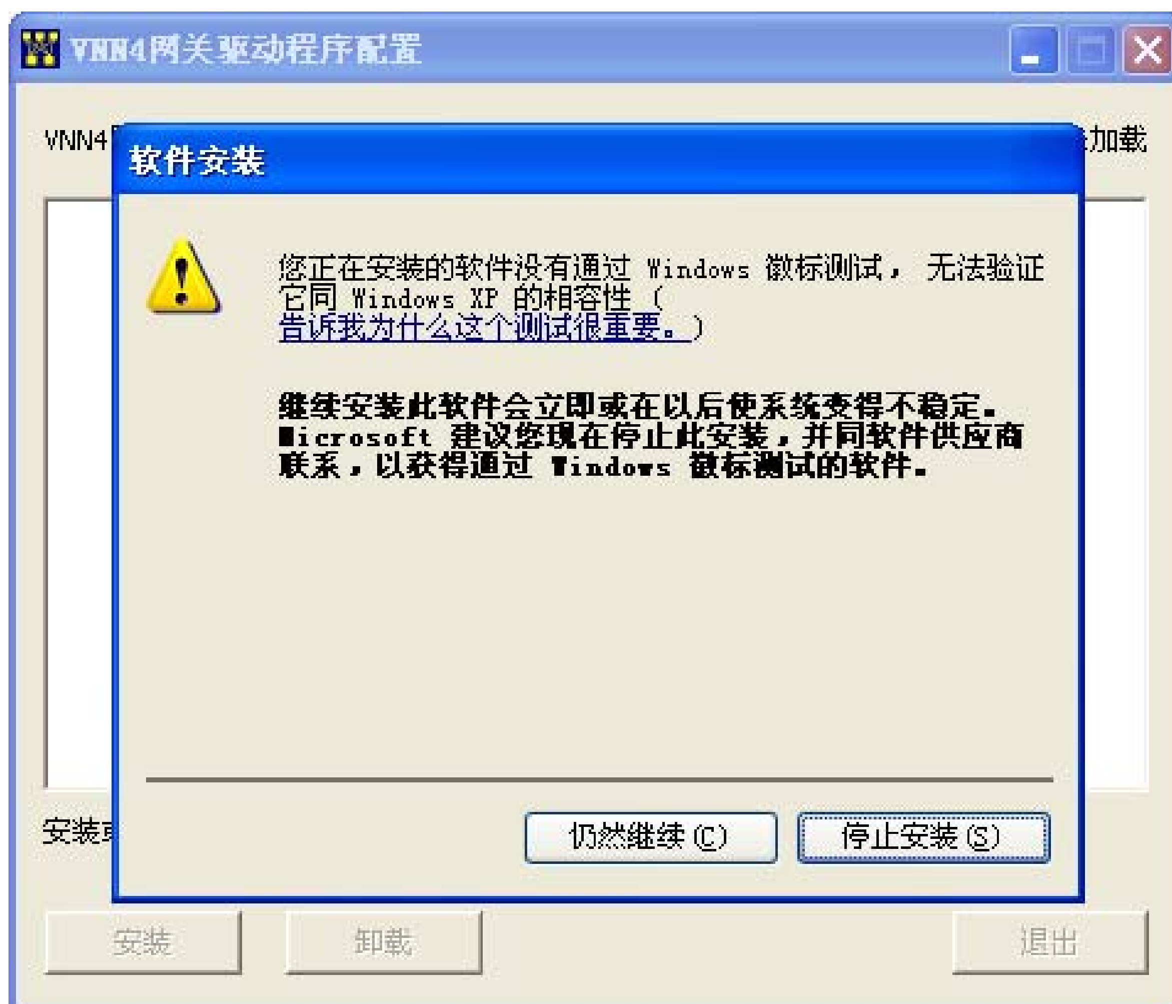
在开始使用网关 NAT 转发功功能前，您需要先对您充当 NAT 网关功能的计算机进行适当的安装和配置。您需要先将您的 VNN 客户端设置成网关模式，并登陆一个网关帐号。

当帐号登录成功后，点击“配置”选项卡，然后在页面底部找到“NAT 配置”，并点击对应右侧的“配置”按钮。如下图：



如果您没有安装过网关 NAT 的驱动程序，需要先点击“启动 NAT 的驱动配置”连接，在出现的对话框中点击“安装”按钮，并稍等片刻。

※注意：在安装的过程中，您的 Windows 可能会提示即将安装的驱动程序未通过 Windows 徽标认证，请务必点击“仍然继续”按钮。否则可能会导致安装失败。



当驱动程序安装完毕后，点击退出按钮即可。

※注意：在安装完驱动后，界面可能会返回登录状态，您需要登录帐号才可以返回到之前的配置界面。

Chapter 5

再次进入登录界面后，您将会看到类似以下的界面，它被称为网关 NAT 转发列表：

NAT 配置

安装情况 运行情况

NAT安装和卸载：

点击下面的链接启动NAT安装和卸载程序。安装和卸载过程中，网络将中断， VNN界面也将重新退出。 仅有本地访问才能配置。

启动nat的驱动配置

	VNN地址	映射Ip	

只有点击"提交"按钮收到成功的返回时，修改的配置才会被保存生效。

刷新 添 加 修 改 删 除 清除 提 交 取 消

通过点击“刷新”按钮，可以同步本地缓存与界面中的内容，点击“添加”按钮可以添加一条新的网关 NAT 转发策略。选中一条策略并点击“修改”按钮可以修改一条已经添加的策略，“删除”按钮则是删除已经选中的一条策略，点击“清除”按钮则会清除掉列表中的所有内容。当设置完毕后，需要点击“提交”按钮才能够生效，点击“取消”则会放弃当前的修改。

现在，如果需要添加一条到 IP 为 192.168.1.80 的网络打印机的网关 NAT 转发，首先点击“添加”按钮，选择一个 VNN 的 IP 地址，然后在下方的 IP 地址中填写网络打印机的物理 IP 地址，并点击确定按钮即可。

添 加

虚拟地址： 2.2.77.201

映射Ip 192.168.100.100

确 定 取 消

当确定后，您将会返回之前的网关 NAT 转发列表界面，并且看到您刚才添加的策略信息：

	虚拟地址	映射Ip	
1	2.2.77.201	192.168.100.100	

如果您需要添加多条策略，可重复以上步骤，如果输入的映射 IP 地址有误，可选中有误的策略，并点击“修改”按钮即可进行修正。

当您添加完您所需的转发清单后，通过点击提交就可以使转发列表立即生效了。

您可以在其他远端的 VNN 客户端登录一个同组的其他普通帐号，然后访问该该网络打印机(192.168.1.100)对应的 VNN 地址 2.2.77.201，即可通过网关 NAT 转发访问到该设备。

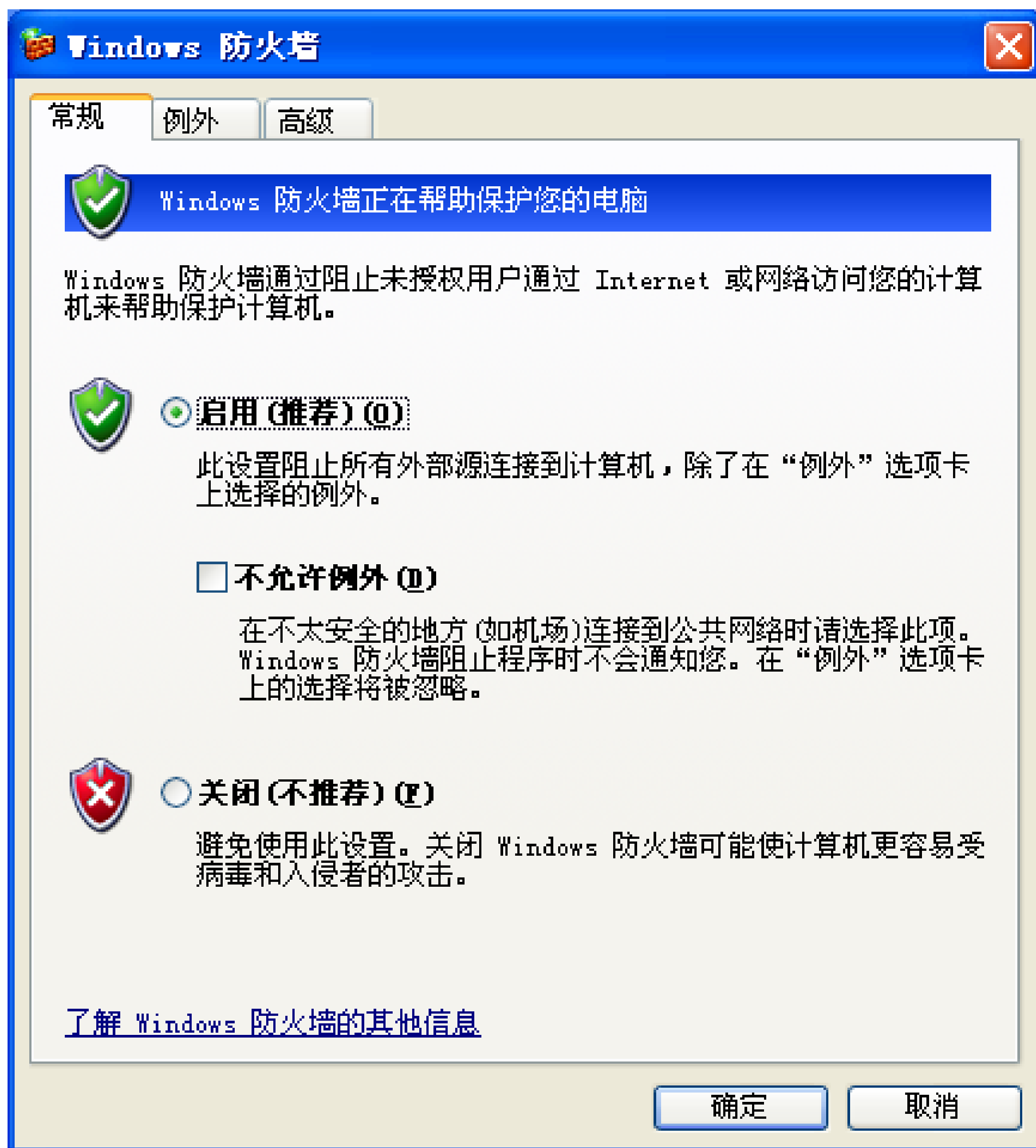
Chapter 6

VNN 与个人主机防火墙

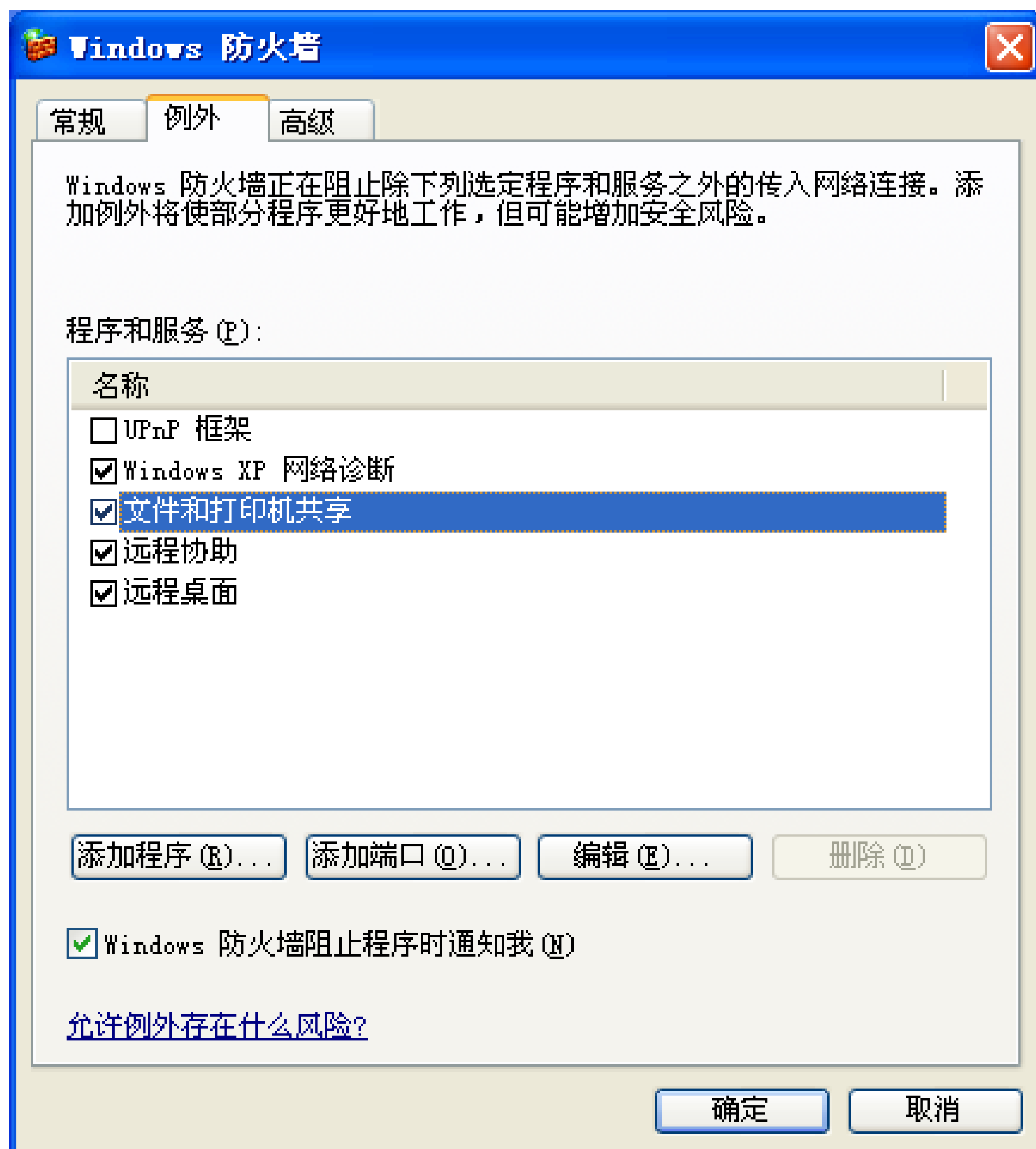
Chapter 6

一．配置Windows XP网防火墙允许通过VNN访问文件共享

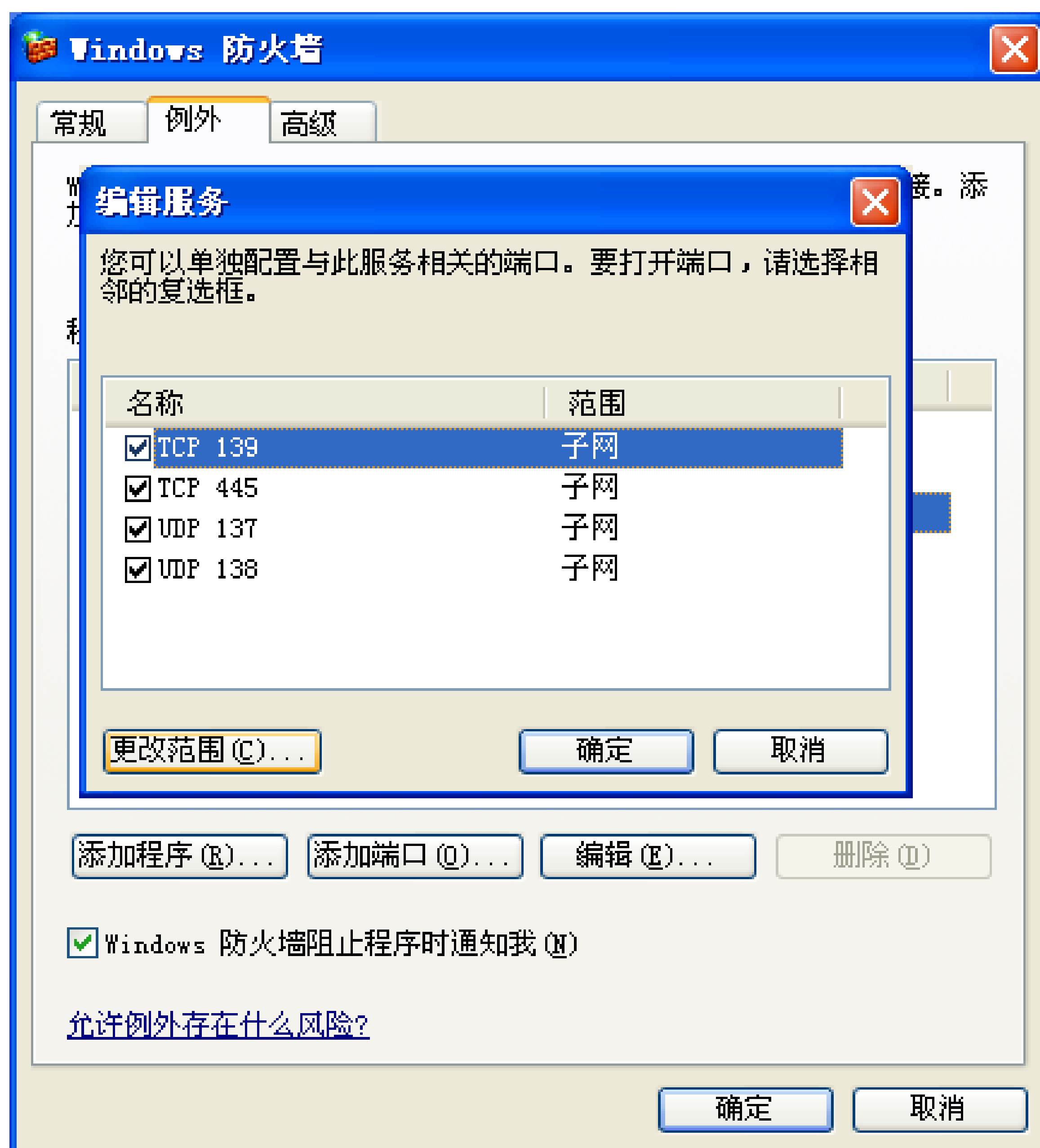
点击开始菜单，进入控制面板，点击“Windows 防火墙”即可看到以下界面：



点击例外选项卡，并选中“文件和打印机共享”，然后点击“编辑”按钮。

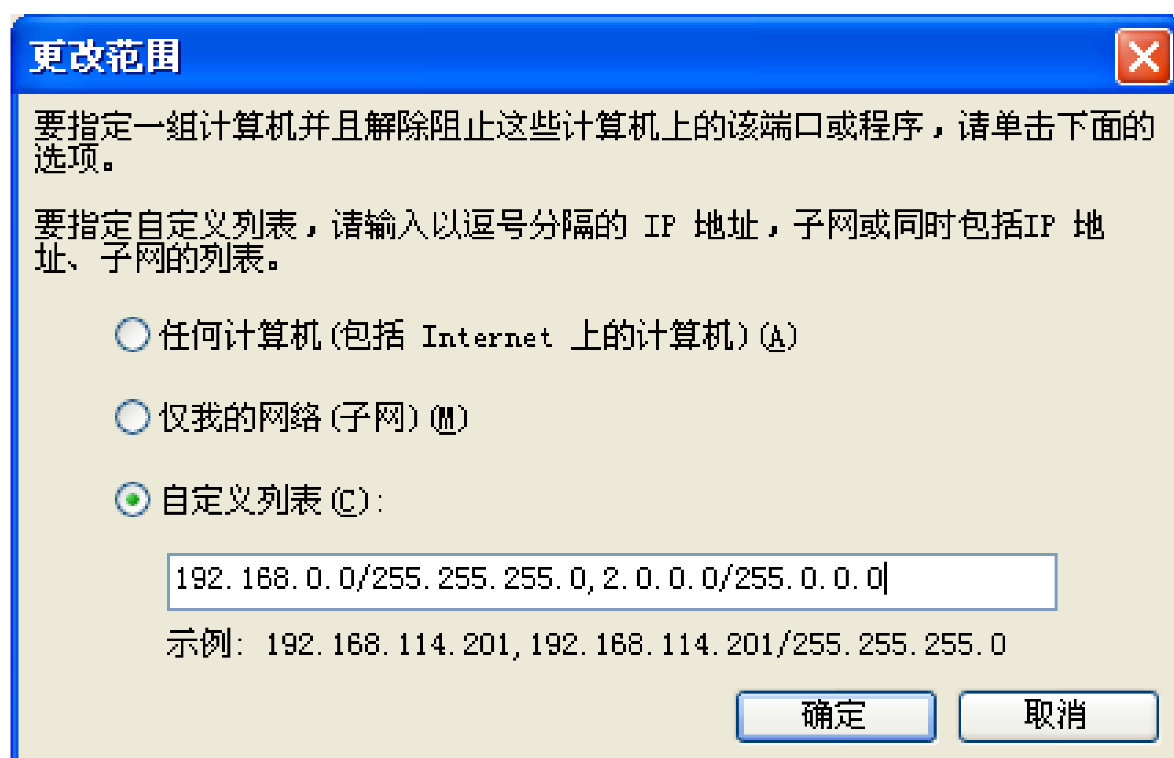


在出现的编辑服务对话框中，选中“TCP 139”，并点击“更改范围”按钮。



在出现的更改范围对话框中输入您的局域网 IP 地址范围和 VNN 的 IP 地址范围。

注意：如果您不希望局域网中访问到您的共享，那么请直接填写 VNN 的网络 IP 范围即可。VNN 的 IP 地址范围是 2.0.0.0/255.0.0.0 。



二．针对VNN4 配置瑞星防火墙

第一步：右击任务栏右下角的瑞星防火墙图标，选择“详细设置”出现如下界面：



第二步：在列表的左侧选择规则设置下的白名单选项，然后点击右侧的“增加”按钮。3

在新出现的增加白名单对话框中，从地址类型选择：“地址范围”，然手输入（如下图）：

起始地址： 2.0.0.0
结束地址： 2.255.255.255

点击确定按钮，即可看到刚才添加的策略已经出现在列表中了。再次点击确定按钮关闭设置对话框。

第三步：双击任务栏右下角的瑞星防火墙图标，出现如下界面：



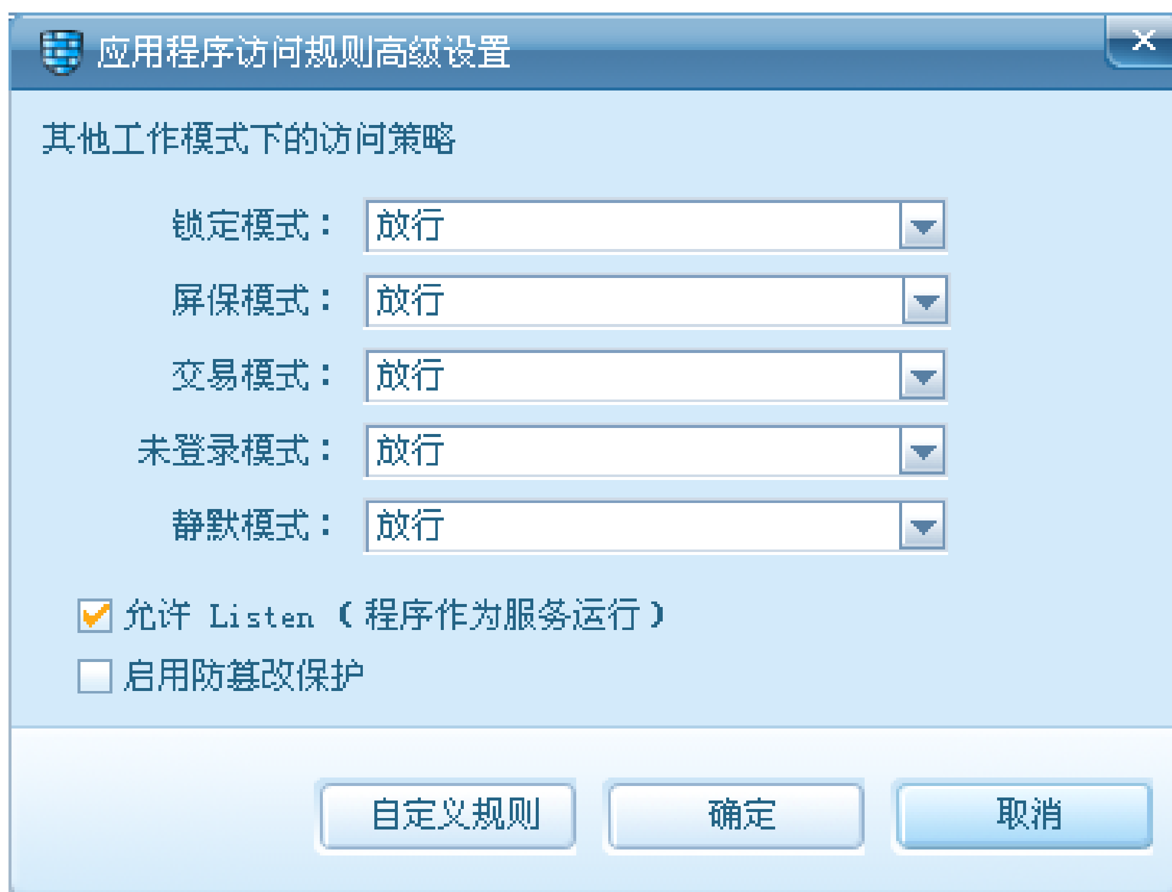
第四步：点击工具条上的“访问控制”标签，出现如下界面：



第五步：在出现的访问控制列表中点击“增加”按钮，会要求您选择应用程序，请在路径里输入：
C:\Program Files\Common Files\VNNShared\VNN Core Engine Service\VNN4CSRV.exe
并点击确定按钮，出现如下界面：



第六步：将“常规模式”选择“放行”后，点击“高级”按钮，会出现以下的对话框：



确保都是放行以后，点击“确定”按钮，即可完成设置。

三．针对VNN4 配置卡巴斯基(KAV)7.0 互联网安全套装

（**此处以 KAV 互联网安全套装 7.0 为例，注意普通的 KAV 防病毒版本无此问题）

如果将 VNN 安装在有 KAV 互联网安全套装的机器上会出现此 PC 的应用不能被远程 VNNPC 正常访问的问题。

分析原因如下：由于 VNN 各端互联使用了 2.0.0.0 网段进行通讯，这个网段是国际互联网组织（ICSA）的保留地址不分配给公网用户，但是某些防火墙软件安全性高不允许 2 网段主机与本地主机通讯。为了避免这一现象，请按如下步骤进行操作即可解决问题。

第一步：打开本地 KAV 管理界面，点击防火墙，在右侧点击过滤规则(如下图所示)



第二步：在区域选项卡理点击“添加”按钮，增加 VNN 的地址范围，如下页图所示



第三步：在区域设置理添加 VNN 的网段 2.0.0.0——255.0.0.0，点击选择“信任的”，最后点击“确定”按钮后即可解决问题。



设置结果如下图第一行所示：



四．设置卡巴斯基KIS2009 使用VNNIP进行远程桌面的操作

版本：卡巴斯基全功能安全软件 2009

当卡巴斯基 2009 执行默认安装后，会自动开启防火墙并阻止使用登陆 VNN4 获得的 IP 地址来进行远程桌面，为了使用 VNN4 的 IP 地址来进行远程桌面的操作，需要做如下设置：

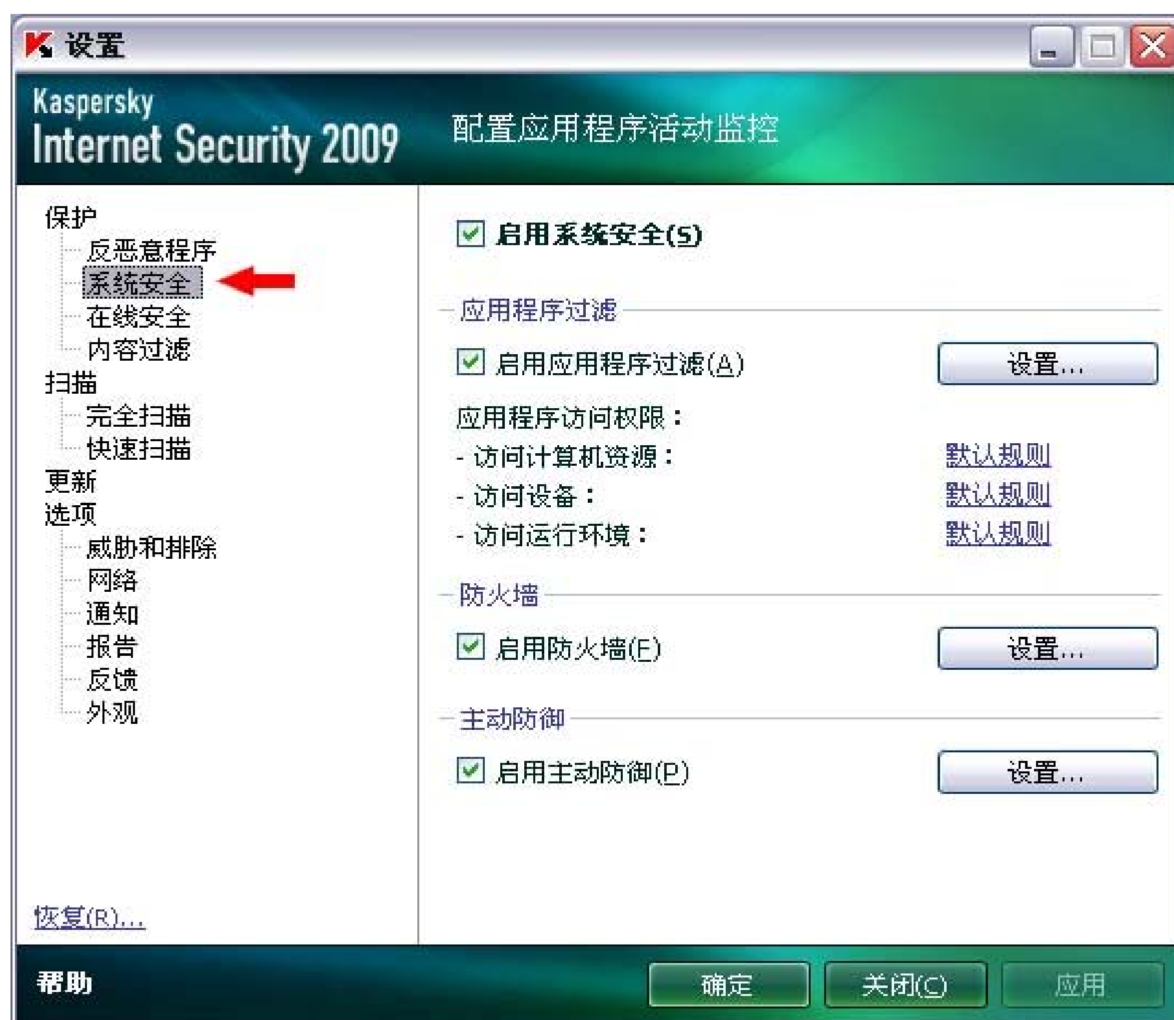
打开卡巴斯基 2009 程序的主界面，如下图



点击设置按钮，出现下图

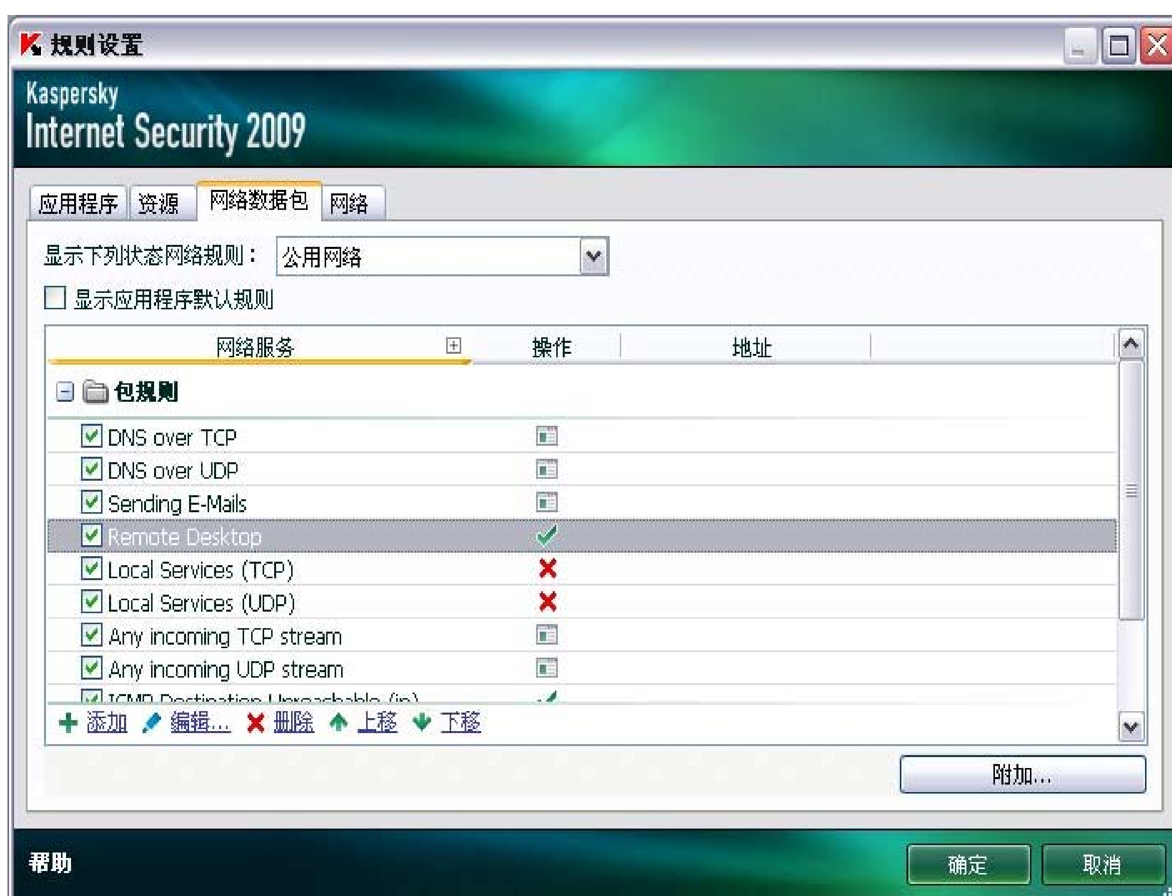

设置
Kaspersky
Internet Security 2009
配置常规保护设置
保护
反恶意程序
系统安全
在线安全
内容过滤
扫描
完全扫描
快速扫描
更新
选项
威胁和排除
网络
通知
报告
反馈
外观
恢复(R)...
启用保护(E)
计算机启动时运行卡巴斯基全功能安全软件(L)
交互式保护
选择自动操作(A)
不删除可疑对象(S)
密码保护
启用密码保护(P)
设置...
管理设置本程序
加载...
保存...
恢复(R)...
帮助
确定
关闭(C)
应用

点击系统安全选项，内容如下图



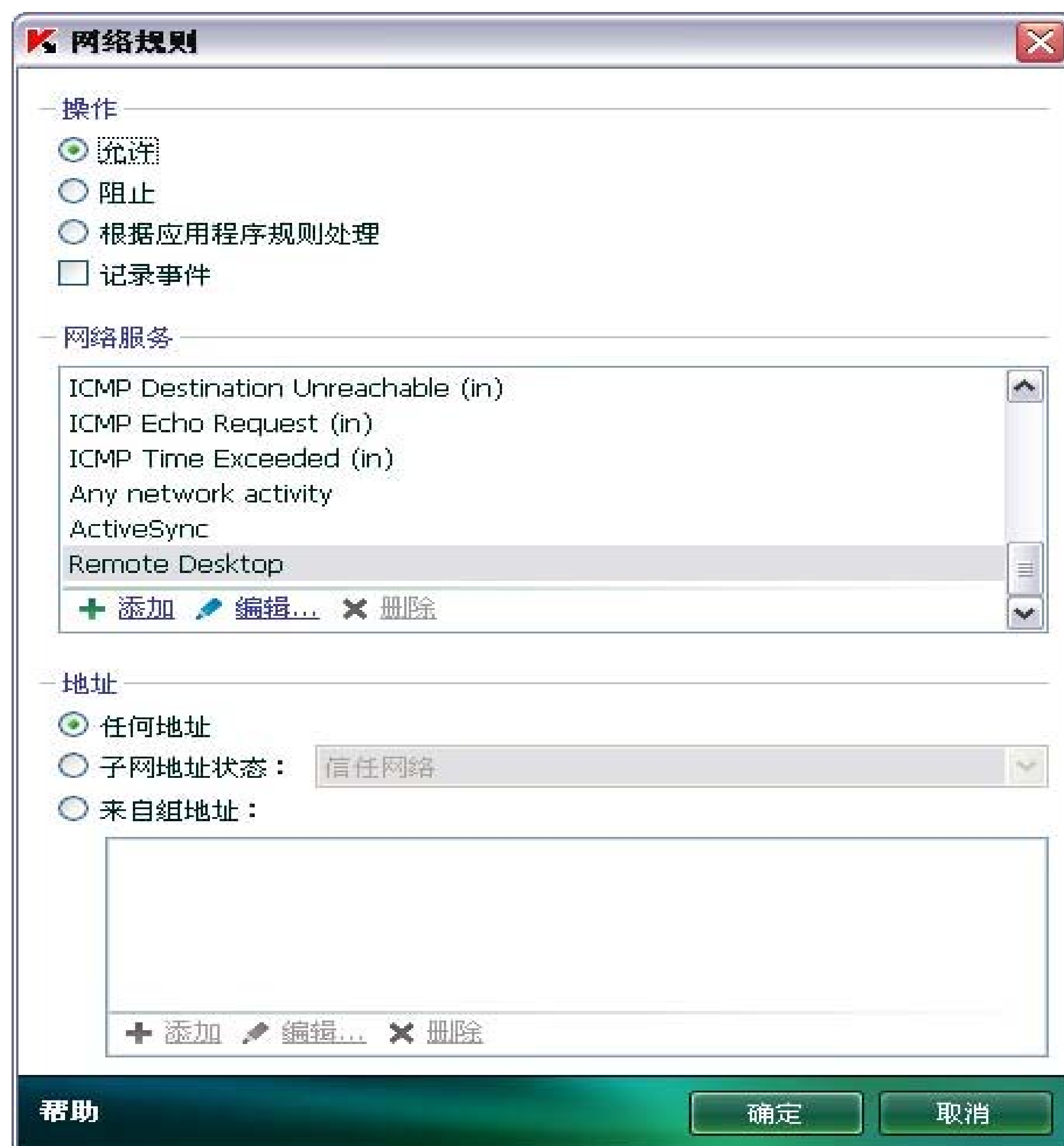
Chapter 6

VNN4 的相关应用程序会自动被应用程序过滤放入低限制组中，不会被过滤掉，所以不需要额外的设置。无法通过 VNN 的 IP 远程桌面的问题是因为在卡巴斯基 2009 防火墙的规则设置中没有在公有网络中允许远程桌面点击防火墙右侧的设置按钮，如下图所示：



选择“显示下列状态网络规则中”下拉菜单的公用网络

点击包规则下的 Remote Desktop 选项，选择编辑，按下图所示配置



点击确定后，就可以使用登陆 VNN 获得的 IP 地址进行远程桌面的操作了。

五．针对VNN配置金山网镖

首先打开金山网镖的配置界面，点击“应用规则”选项卡：



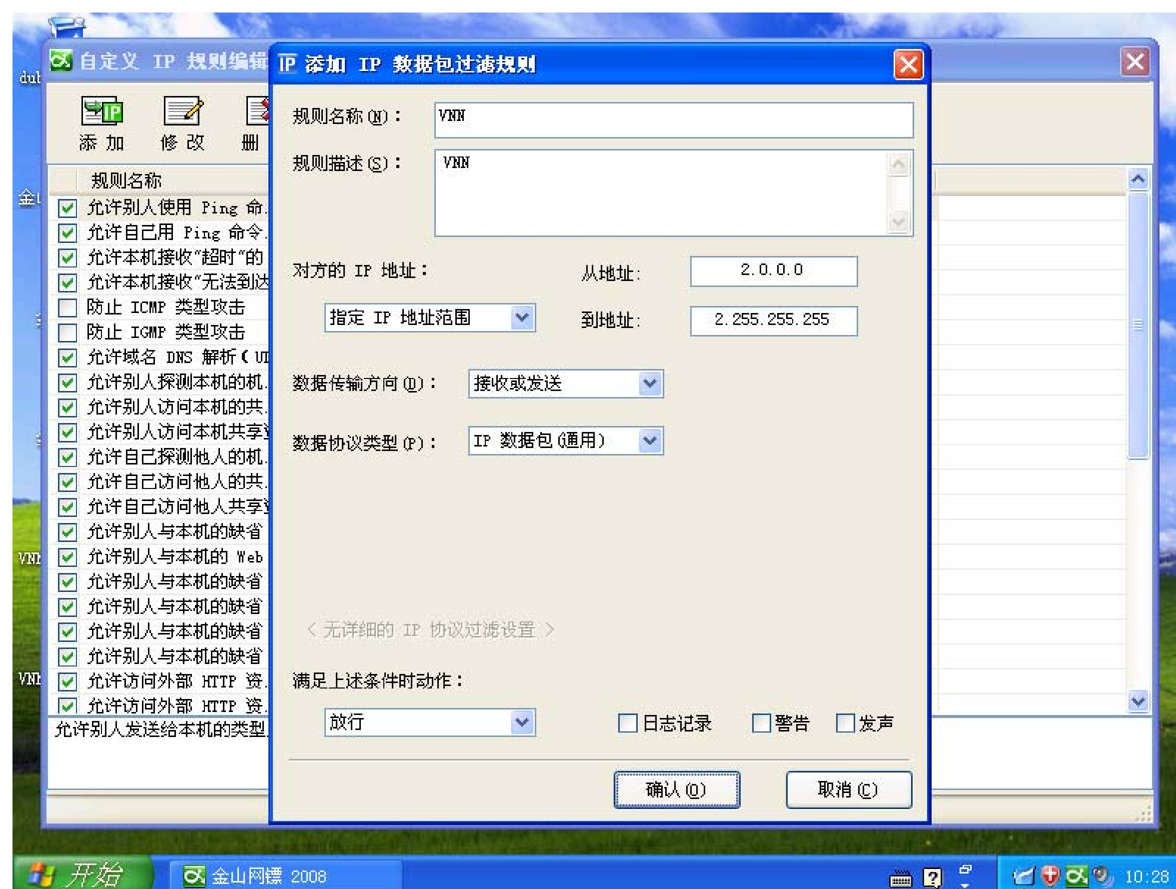
点击在列表中找到 VNN Core Engine Service 和 VNN Core Engine Monitor ，然后将对应的右侧选项设置为“允许”（如上图）。

然后，转到“监控状态”选项卡（如下图）：

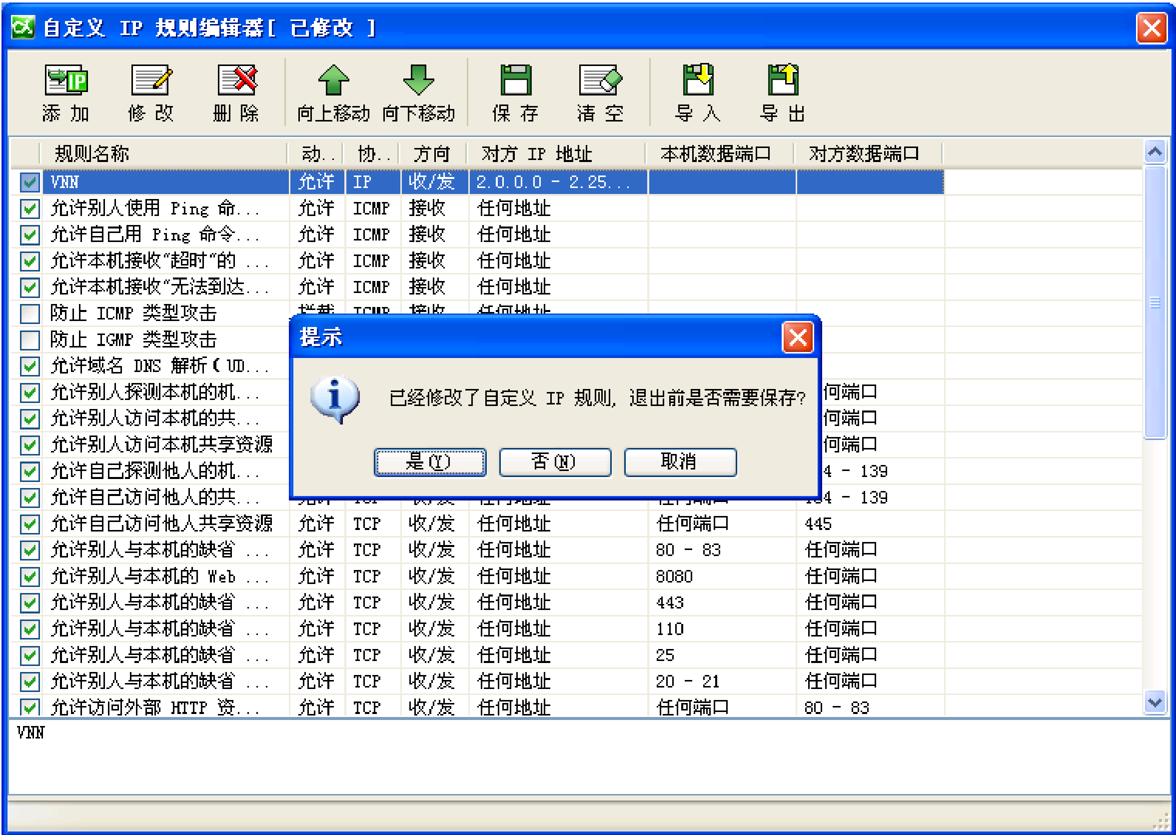


点击“互联网监控”右侧的“详细设置”连接。

在新出现的自定义ＩＰ规则编辑器中点击“添加”按钮，然后在出现的添加 IP 数据包过滤规则对话框中按照以下图片所述进行配置：



配置完成后点击确定按钮，并点击保存即可完成配置。



注意：请确保新添加的策略位于规则列表的最上层。如果没有位于最上层，请选中 VNN 的策略，并点击向上移动按钮移至最顶端。

Chapter 6

六．针对VNN4 配置趋势科技网络安全专家 2009

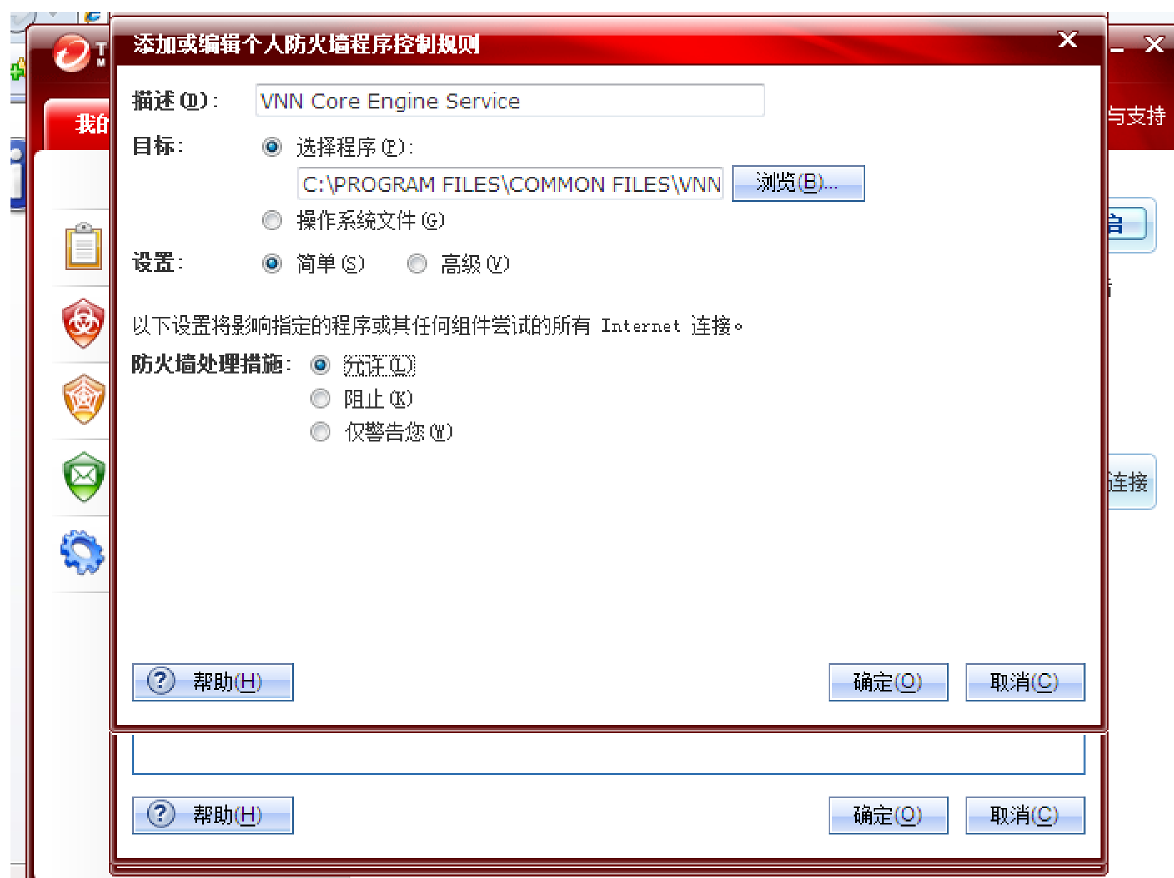
首先，双击任务栏右下角的趋势科技网络安全专家２００９图标，在出现的控制台界面中点击“个人防火墙控制”，并点击“设置”链接，如下图：



在新出现的个人防火墙配置文件高级设置对话框中点击“程序控制”，找到 VNN Core Engine Service ，选中并点击“编辑”按钮。



在新出现的“添加或编辑个人防火墙程序控制规则”中，将其按照下图的选择进行配置：



配置完成后，点击确定按钮返回上一个对话框。

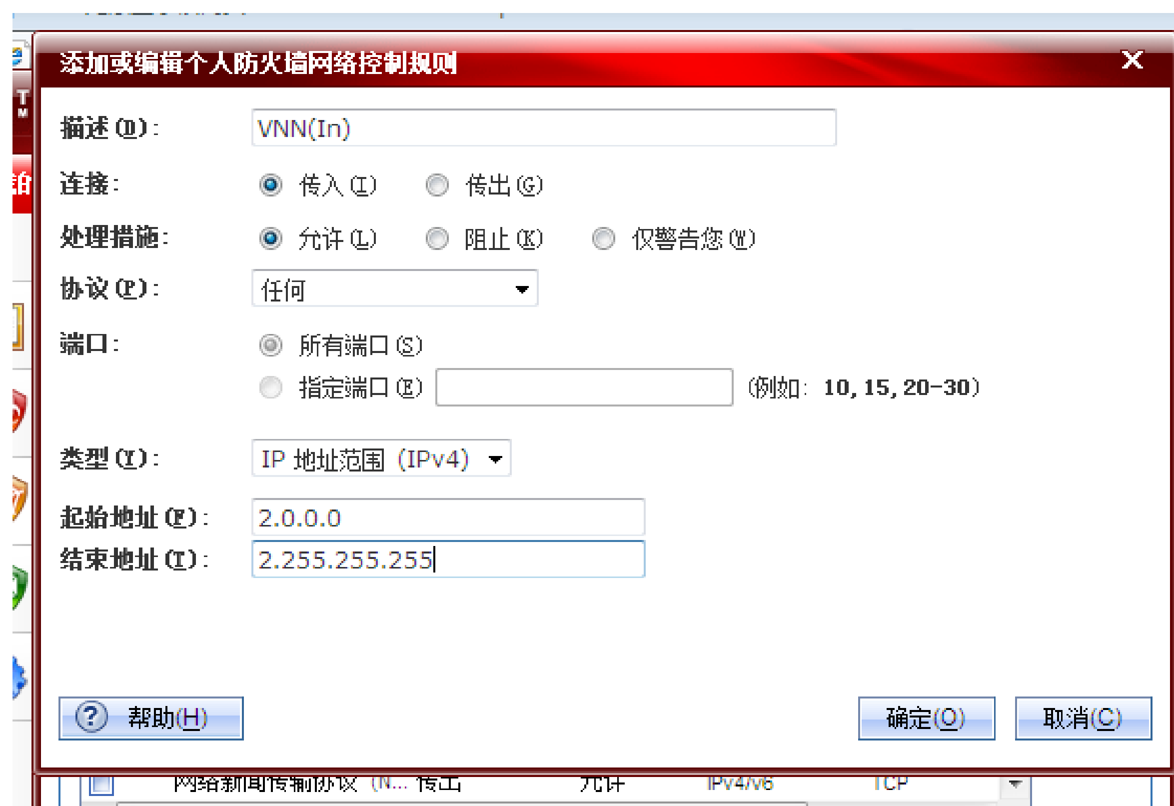
返回“个人防火墙配置文件高级设置”对话框后，点击“网络协议控制”对话框，并点击“添加”按钮。



在新出现的“添加或编辑个人防火墙网络控制规则”中，按照以下设置进行配置：



配置完成后，点击确定按钮，并再次点击“添加或编辑个人防火墙网络控制规则”对话框中的添加按钮。然后再次按照下图的配置进行配置：



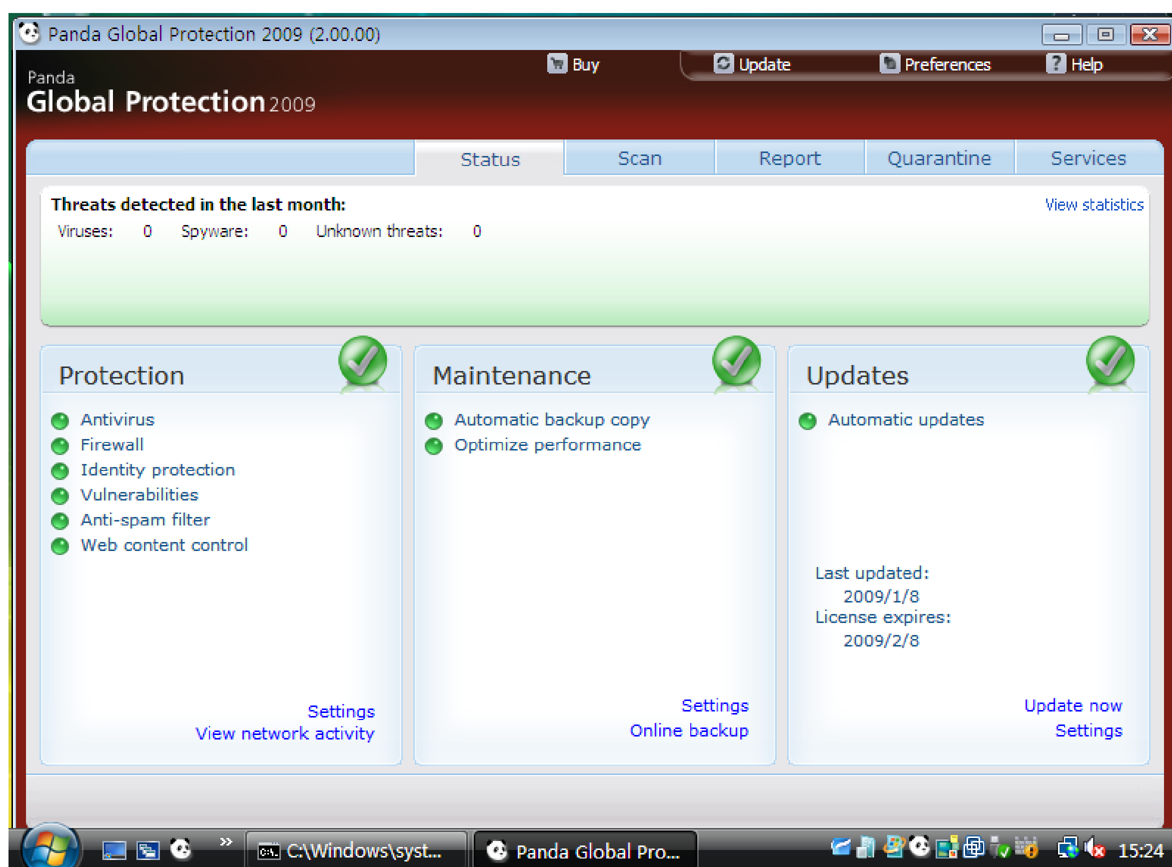
点击确定后，显示应该如下图所示：



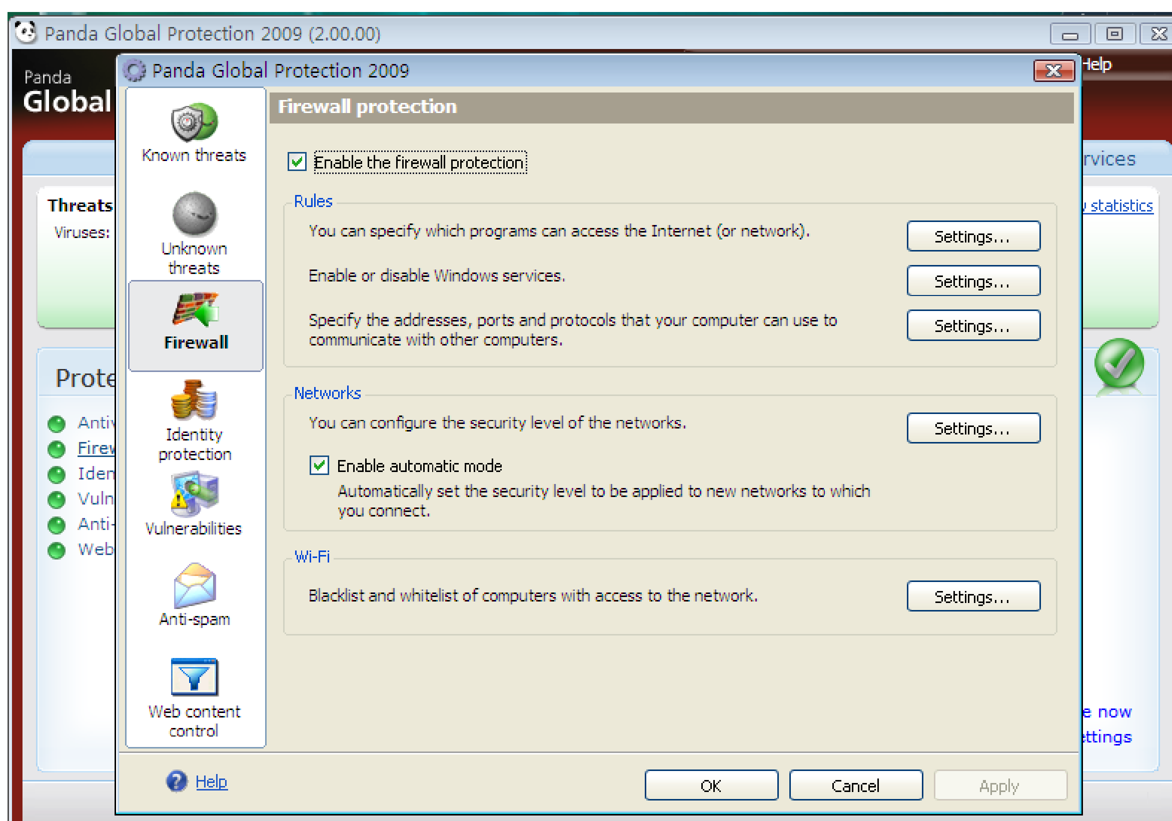
确认无误后，点击确定按钮，即可完成配置过程。

七．针对VNN配置熊猫全面防御 2009

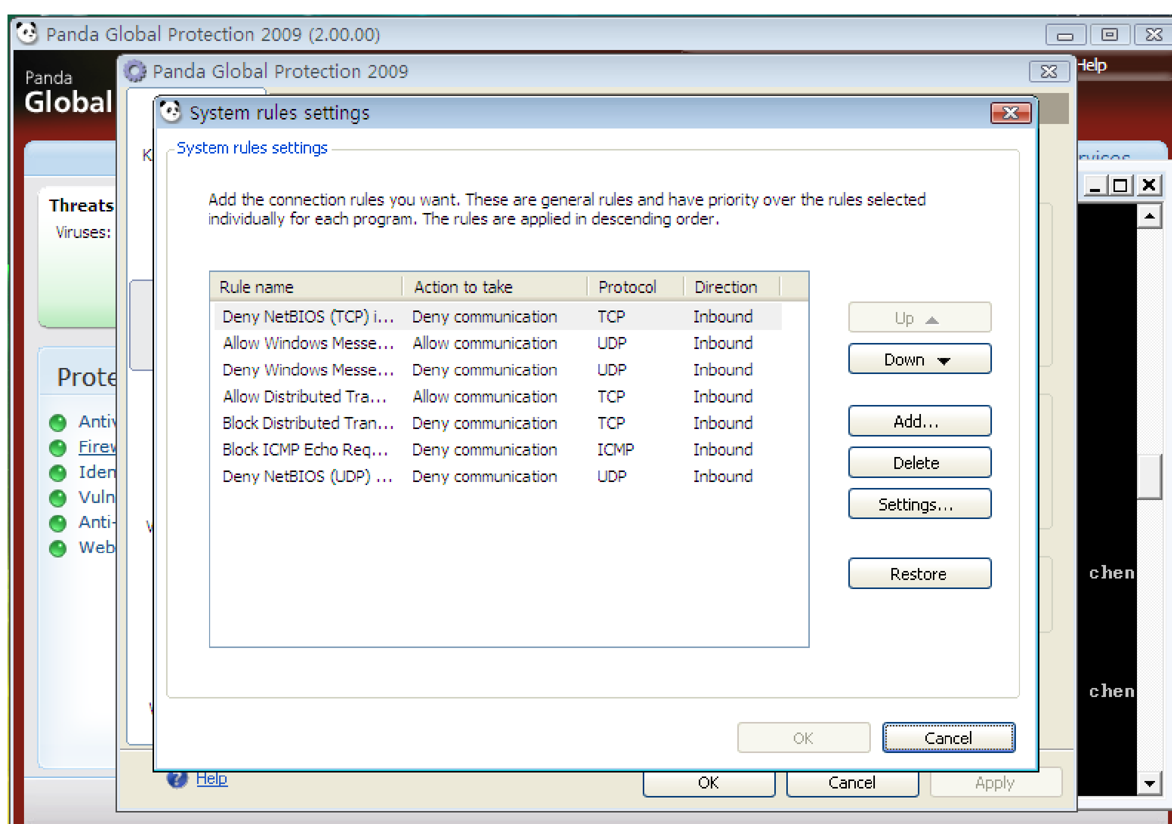
首先，双击任务栏右下角的熊猫图标，将会出现如下图所示的界面：



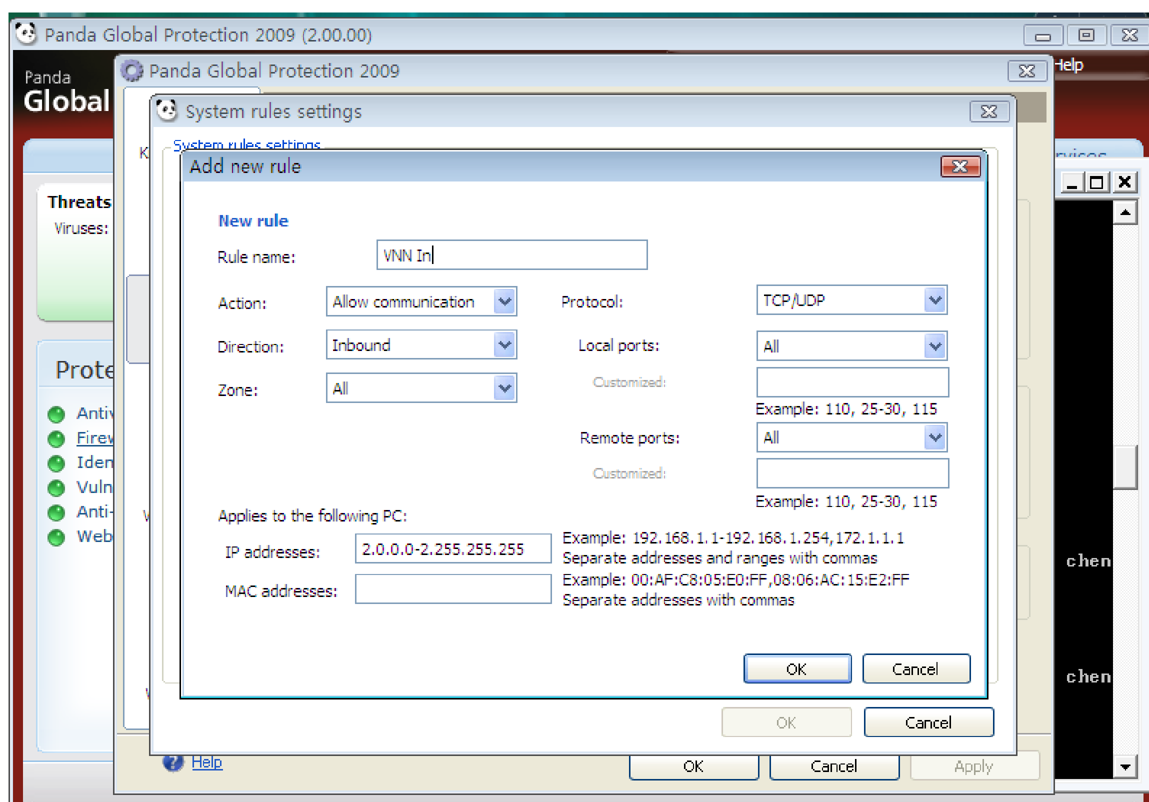
点击 Protection 下的 Firewall 连接，将会出现如下图的新窗口：



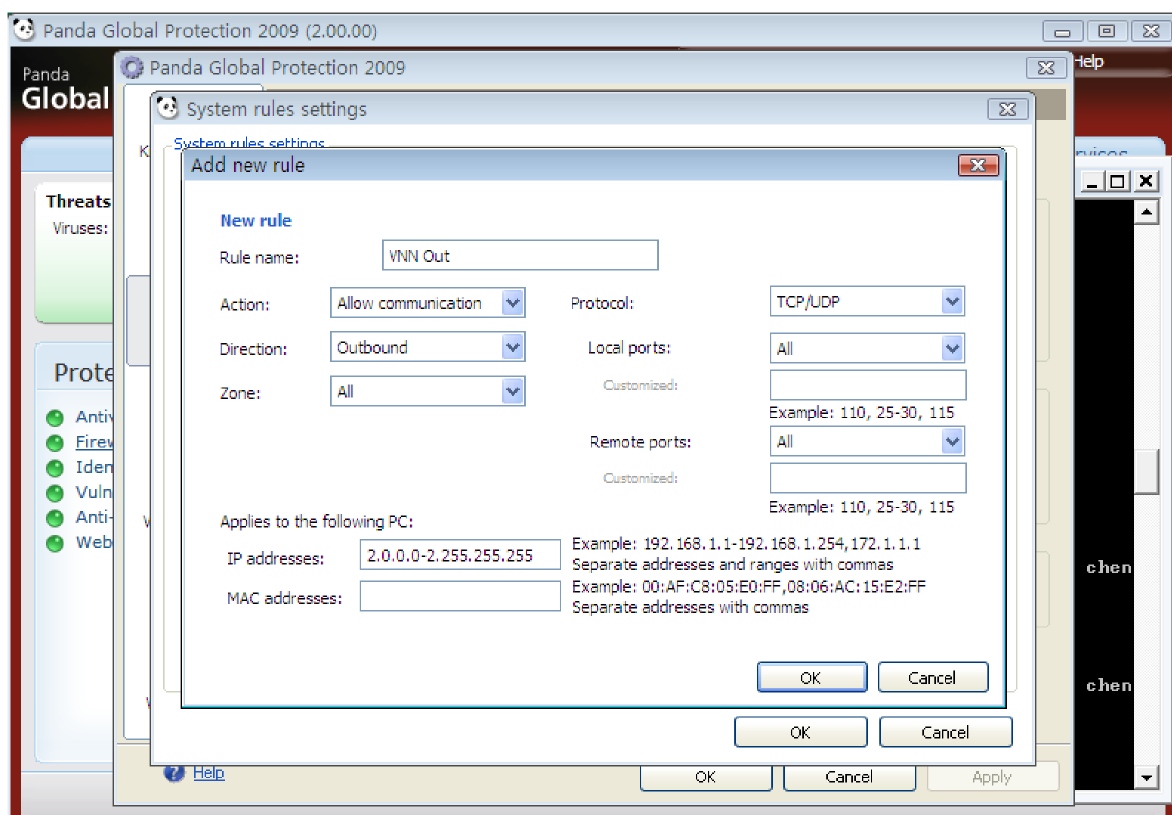
在上图的窗口中，点击 Specify the Addresses, Ports and Protocols ...该行英文右侧的 Settings... 按钮，将会出现如下图的新窗口：



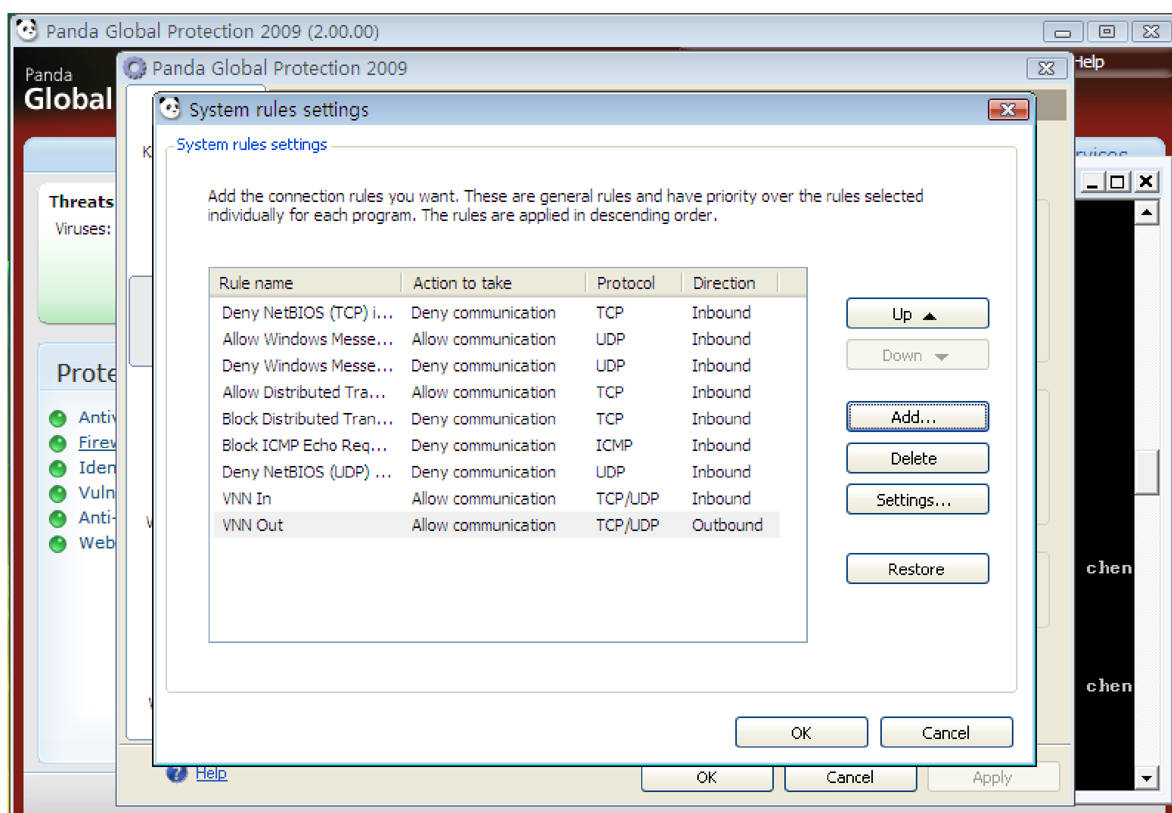
点击“Add...”按钮来添加一条新的规则以允许ＶＮＮ的应用正常进行，请按照下图的设置进行配置：



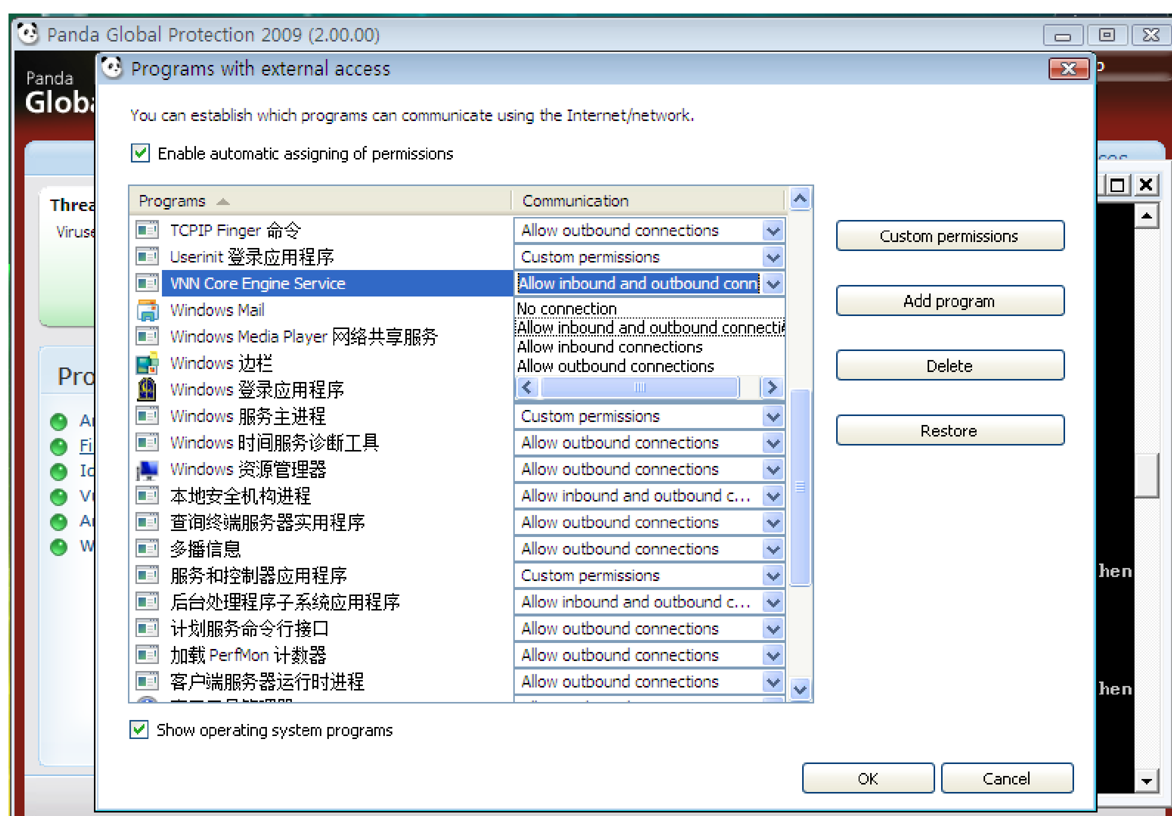
设置完成后，点击 OK 按钮，然后再次点击“Add...”按钮，填写如下图所示的另一条规则：



完成后点击 OK 按钮，返回到 System Rules Settings 界面，正常情况，应该多出如下图的两条规则：



确认无误后，点击 OK 按钮，然后再次点击“You Can Specify Which Programs...”英文右边的 Settings...按钮，将会出现以下界面：



选中下方的 Show Operating System Programs 复选框，然后找到 VNN Core Engine Service，从右侧的 Communication 下拉列表中选择 Allow Inbound and outbound connections。

设置完毕后，点击 OK 按钮即可完成全部配置。

Chapter 7

VNN4 常见问题解答

1.安装问题

1.1.在安装时遇到“处理器类型错误”
1.2.在安装过程中提示“访问被拒绝”
1.3.在安装过程中，计算机安全保护软件提示VNN4CSRV.EXE正在试图安装内核驱动

2.注册问题

2.1.在启动VNN界面时出现提示“不能连接到VNN SN服务器”
2.2.在尝试注册组时提示“创建组出错：超时”
2.3.在注册的过程中提示“资源不可达，请检查你组的最大用户数”

3.登录问题

3.1.如何配置网络防火墙或路由器/网关中的防火墙以允许VNN4 正常使用
3.2.在登录时遇到“您现在无法连接到探测服务器！”警告提示
3.3.在登录某个特定的组成员帐号时提示该成员过期

4.使用问题

4.1.如何修改密码
4.2.如何限定一个帐号的截至日期
4.3.我在完成续费后显示仍然是即将过期或原有的到期日期
4.4.如何开启网络加速(WOC)功能
4.5.不停的出现“VNN Core Engine 发生错误并意外退出”

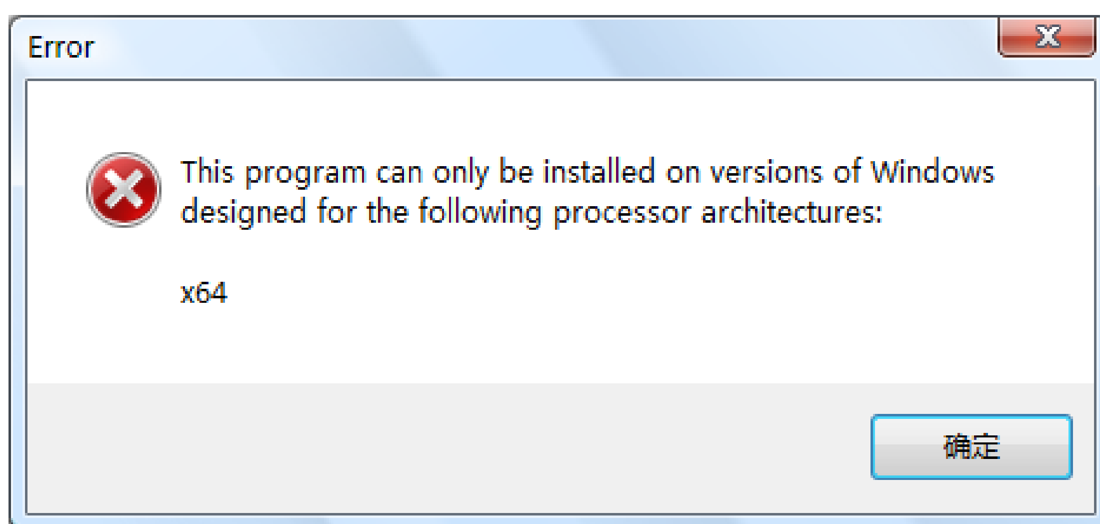
5.应用问题

5.1.无法PING通对方
5.2.无法通过VNN进行远程桌面
5.3.无法通过VNN进行SQL Server数据库连接
5.4.无法访问对方的文件共享

Chapter 7

1.1.在安装时遇到“处理器类型错误”

当用户在计算机上试图安装 VNN 时遇到以下错误提示：



该问题是由于用户选择的安装包的版本与操作系统的版本不符导致的。如果您的操作系统是 64 位(x64)，则应该选择 64 位的 VNN4 安装程序。

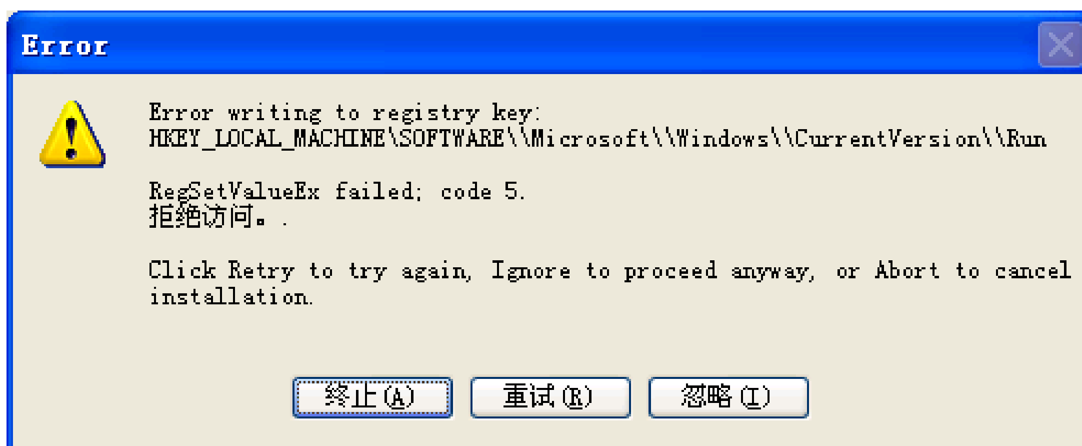
如果您的操作系统是 32 位(x86)，则应该选择 32 位的 VNN4 安装程序。

请查看您操作系统所附带的帮助文件以核对您的操作系统版本，对于 Windows 用户，请点击开始菜单，选择运行，然后输入 winver 并回车或点击“确定”按钮核对自己的操作系统版本。

请检查VNN4 的安装光盘上的VNN4 客户端版本并选择正确的版本再次安装或访问 http://www.bizvnn.cn 下载对应操作系统版本的VNN4 客户端。

1.2.在安装过程中提示“访问被拒绝”

在某些特定软件环境的计算机上，安装 VNN4 的过程中可能会出现如下图的提示：



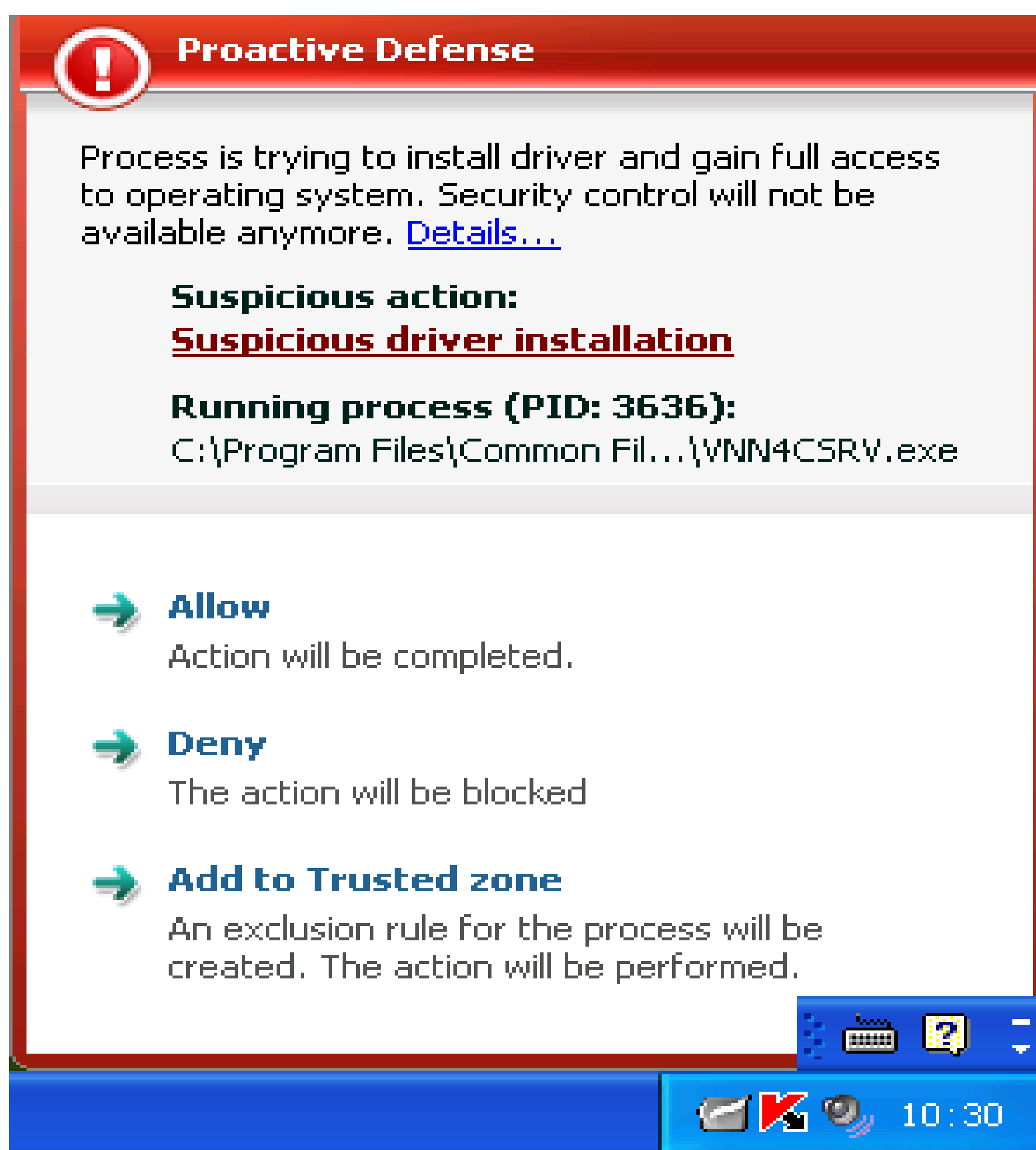
如果出现该错误，通常情况下是由于用户在没有管理员权限的用户中按安装导致的。请检查当前登录操作系统的用户是否具有 Administrator 权限或是否位于 Administrators 用户组。

另外，在安装有 McAfee 计算机安全保护软件的软件环境上，在启动特定的 McAfee 安全设置的情况下也会遇到以上问题。请联系您的 McAfee 安全保护软件的供应商以寻求解决办法或暂时关闭/退出您的 McAfee 安全保护软件，然后再次点击“重试(R)”按钮继续安装。

1.3.在安装过程中，反病毒软件主动防御功能提示 VNN4CSRV.EXE 正在试图安装内核驱动

在某些特定软件环境的计算机上，安装 VNN4 的过程中安全保护软件的主动防御功能可能会得到如右图的警报提示。

为了确保 VNN4 的顺利安装，如果您遇到了类似右图的提示，请点击 Allow (允许)或 Add to Trusted zone (添加到可信任区域)按钮以继续 VNN4 的安装。



2.1.在启动 VNN 界面时出现提示“不能连接到 VNN SN 服务器”

在某些特定的网络环境或软件环境中启动 VNN 后，可能会出现如下图的对话框。



如果出现该提示，意味着一下三种可能性，请您依次进行排查：

1.VNN4 的服务器可能处于维护状态。

您可以访问 http://www.bizvnn.cn 检查有无VNN4 服务器的维护公告，并稍后再次尝试登录。

2.您的网络防火墙未允许 VNN4 访问互联网。

如果当前的计算机存在网络防火墙，请检查您的网络防火墙配置，并将位于“C:\Program Files\Common Files\VNNShared\VNN Core Engine Service\VNN4CSRV.exe”(不包含引号)或将 VNN4CSRV 服务添加到您防火墙的白名单或例外规则中。

3.您所在的网络需要设置代理才能够访问互联网。

请向您的网络供应商或网络管理员进行咨询，并要求获得您所在网络中的 SOCKS5 代理服务器的相关设置信息。

当您获得了 SOCKS5 代理服务器的配置信息后，请双击桌面上的“VNN-Enterprise Console”，点击右上角的“帮助”连接，再点击“选项”，选中“启用 Socks5 代理”复选框，并且填写您网络供应商或网络管理员所提供的信息，最后点击“设置代理”按钮即可。

※注意：VNN4 目前只支持SOCKS5 代理，SOCSK4、SOCKS4a以及HTTP代理都不被支持。您可以留意我们的官方网站： http://www.bizvnn.cn 查询更新信息。

Chapter 7

2.2.在尝试注册组时提示“创建组出错：超时”

当用户在尝试注册新组时提示“创建组出错：超时”，通常情况下该问题是由于 VNN4 无法访问网络或服务器处于维护状态导致的。请参看 2.1 节内容：《在启动 VNN 界面时出现提示“不能连接到 VNN SN 服务器”》

2.3.在注册的过程中提示“资源不可达，请检查你组的最大用户数”

当用户注册了一个网关帐号时并且子网用户数量过多时可能出现该问题。

如果您不清楚网关帐号的具体作用，请不要选中“网关帐号”复选框，否则很有可能导致该组内成员的剩余数量被全部耗尽。

我们建议用户在我们的技术人员的指导下创建和使用网关帐号。您可以在 http://www.bizvnn.cn 获得我们技术人员的联系方式。

3.1.如何配置网络防火墙或路由器/网关中的防火墙以允许 VNN4 正常使用

一般情况下，对于本地软件网络防火墙，建议用户将“C:\Program Files\Common Files\VNNShared\VNN Core Engine Service\VNN4CSRV.exe”(不包含引号)或将 VNN4CSRV 服务添加到您防火墙的白名单或例外规则中。这样能够让 VNN4 发挥最大效果。

对于网关或硬件防火墙，您应该遵循以下策略：

允许安装了 VNN4 的计算机的 IP 地址能够访问任何互联网/内网地址的任何目标，包括双向访问。

3.2.在登录时遇到“您现在无法连接到探测服务器！”警告提示

在某些存在网络显示的情况下，当用户登录时，可能会遇到：“您现在无法连接到探测服务器！如果您现在仍然能够上网，请检查防火墙是否允许了 VNN 必须的 UDP 端口。”的警告提示。

如果出现该提示，则意味着您的网络可能存在封锁或防火墙配置有误。如果是防火墙问题，请参看 2.1 章节的第 3 小节部分。

3.3.在登录某个特定的组成员帐号时提示该成员过期

当登录某个特定的组成员帐号时，提示该帐号已过期。但是该组中的其他成员正常。

该问题是由于组管理员给当前帐号设定了过期日志导致的。请联系您的组管理员取消限制或询问具体原因。

解决该问题需要以组管理员的身份登录该组并进行相关操作。具体的步骤是：

以组管理员的身份登录 VNN4，然后在界面左边的帐号列表中选择登录时提示帐号过期的帐号，然后点击“配置”选项卡，在配置选项卡下方的起始时间和终止时间按照您的需求设定。如果您不希望该帐号在正常使用的情况下过期，则应该选中两个“和本组设置相同”的复选框。

当修改完毕后，点击右边的“提交”按钮即可。

起始时间：

2007-05-25  和本組设置相同

终止时间：

2009-01-01  和本組设置相同

Chapter 7

4.1.如何修改密码

如果是要修改当前已登录帐号的密码，那么您需要通过当前的帐号和密码登录 VNN 的界面，然后在左侧的列表中点击自己的帐号(通常位于第一个)，然后点击配置选项卡，在修改密码中即可修改。最后点击提交按钮即可。

如果您需要修改其他成员的密码，您需要以管理员帐号登录。通常情况下，管理员帐号是以 admin.组名.vnn 的形式出现的。

当您以管理员帐号登录 VNN 后，在左侧的帐号列表中选择需要修改的帐号，再点击配置选项卡即可在修改密码中修改。最后点击提交按钮即可。

4.2.如何限定一个帐号的截至日期

某些时候，可能需要为某位出差的员工限定 VNN 帐号的使用日期。首先，以管理员帐号登录 VNN，通常情况下管理员帐号是以 admin.组名.vnn 的形式出现的。

当您以管理员帐号登录后，在左边的用户列表中选中需要限定使用日期的帐号，再点击配置选项卡，在起始时间和终止时间中点击显示的日期，然后再出现的日历列表中选择您希望设定的日期即可。当设定完毕后，点击提交按钮即可完成设定。

4.3.我在完成续费后显示仍然是即将过期或原有的到期日期

这种情况是由于浏览器的缓存导致的。请在 VNN 的界面中登录 VNN 的帐号，然后点击组信息选项卡，再点击右侧的蓝色刷新箭头（如右图）即可解决该问题。 

.如果仍然显示的是原有的时间或即将到期，请访问我们的网站 http://www.bizvnn.cn 获得技术支持信息。

4.4.如何开启网络加速(WOC)功能

网络加速(WOC)功能是用于提升跨地区／跨国的互联加速功能，目前该功能的申请及使用请访问我们的网站： http://www.bizvnn.cn 。

4.5.不停的出现“VNN Core Engine 发生错误并意外退出”

如果不停的出现该错误，请将“C:\Program Files\Common Files\VNNShared\VHttpdRoot\log”(不包含引号)中的日志发送给我们。您可以将日志以电子邮件附件的形式发送到 support@vnner.com ，或者您可以在 http://www.bizvnn.cn 找到我们技术人员的其他联系方式。

5.1.无法 PING 通对方

当双方的 VNN4 都已经登录并且获得 VNN 的 IP 的情况下，无法控制被控端，请按照以下步骤进行分析。

双击桌面上的“VNN-Enterprise Console”，并用您已经登录的帐号登录。进入界面后，在左边的成员列表中找到被控端的帐号，并检查该帐号文字的颜色是否是橘黄色。如果是，则说明对方在线。如果是灰色或蓝色，则选中它，然后点击“统计”选项卡，并点击“尝试连通”按钮。如果能够立即显示对方的在线信息，则说明对方在线，如果提示“对方不在线”则说明对方的计算机可能关机或者帐号可能被注销下线了。请尝试通过物理接触控制该机器并尝试登录 VNN 帐号。

如果显示用户在线，那么点击开始菜单，选择运行，输入：“ Ping xxx.xxx.vnn ”（不包含引号），其中 xxx.xxx.vnn 是对方的 VNN4 帐号。比如对方的帐号是 home.comp.vnn 的话，则输入 ping home.comp.vnn。输入完成后回车或者点击确定，应该会得到类似于以下的提示：

来自 2.1.51.1 的回复: 字节=32 时间=3ms TTL=64 或 Reply from 2.1.51.1: bytes=32 time=2ms TTL=64

如果您能够得到类似于以上的提示，说明您和对方的 VNN4 连接时正常的，请检查对方的远程桌面是否开启。或者操作系统自带的防火墙是否允许了远程桌面的连入。

如果你得到的提示是：

请求超时。或　Request timed out.

则说明对方的计算机上的第三方防火墙或操作系统自带的防火墙阻止了 VNN 的连接，您需要配置您的网络防火墙以允许远程桌面端口的连入。

5.2.无法通过 VNN4 进行远程桌面

首先您与需要检查 VNN4 的连接是否正常，具体操作请阅读 4.1 章节《无法 PING 通对方》

同时，在通常情况下 Windows 不会允许一个没有密码的操作系统帐号进行远程登录。您需要为您的操作系统帐号设定一个安全的密码。而且，您需要将需要远程桌面的帐号添加到“远程桌面用户”中。

5.3.无法通过 VNN 进行 SQL Server 数据库连接

在 VNN4 中使用 SQL Server 2000 可能会遇到一个问题，即当服务器和客户端都登录 VNN4 后，有可能出现能够通过 VNN4 访问服务器上的其他应用，但是无法连接 SQL Server 2000。

该问题是由于 SQL Server 2000 中自身的一个缺陷导致的。您需要在服务器上的 VNN 登录后重新启动 SQL Server 服务即可解决该问题。

目前将 SQL Server 2000 升级到 SP4(Service Pack 4)可能会解决该问题。

Chapter 7

5.4.无法访问对方的文件共享

首先您与需要检查 VNN4 的连接是否正常，具体操作请阅读 4.1 章节《无法 PING 通对方》。

解决方法:Windows 网上邻居互访的基本条件：

1) 双方计算机打开，且设置了网络共享资源；
2) 双方的计算机添加了 "Microsoft 网络文件和打印共享" 服务；
3) 双方都正确设置了网内 IP 地址，且必须在一个网段中；
4) 双方的计算机中都关闭了防火墙，或者防火墙策略中没有阻止网上邻居访问的策略。

若要解决该问题，请确保工作组中的每台计算机都打开 TCP/IP 上的 NetBIOS 并运行"计算机浏览器"服务。为此，请按照下列步骤操作。

第 1 步：打开 TCP/IP 上的 NetBIOSa. 单击开始，单击控制面板，然后单击"网络和 Internet 连接"。

b. 单击网络连接。
c. 右击本地连接，然后单击属性。
d. 单击 Internet 协议 (TCP/IP)，然后单击属性。
e. 单击常规选项卡，然后单击高级。
f. 单击 WINS 选项卡。
g. 在"NetBIOS 设置"下，单击"启用 TCP/IP 上的 NetBIOS"，然后两次单击确定。
h. 单击关闭关闭"本地连接属性"对话框。
i. 关闭"网络连接"窗口。

第 2 步：启动"计算机浏览器"服务
a. 单击开始，右击我的电脑，然后单击管理。
b. 在控制台树中，展开"服务和应用程序"。
c. 单击服务。
d. 在右边的详细信息窗格中，检查"计算机浏览器"服务是否已启动，右击计算机浏览器，然后单击启动。
e. 关闭"计算机管理"窗口。

XP 的共享需要打开 GUEST 用户，及删除本地安全策略中对 GUEST 用户的访问限制。

Chapter 7

具体操作：

首先用控制面板中的用户帐户将 GUEST 用户启用
然后打开开始--设置--控制面板--计算机管理--本地安全策略"打开"本地安全指派--拒绝从网络访问这台计算机"，将其中的 GUEST 删除。

这样就可以共享了。

因为是家庭组网，基本上没有内部安全问题，建议使用“简单共享”方式进行共享，可以通过菜单栏的“工具”，“文件夹选项”，“查看”，在高级设置里，勾选“使用简单文件共享

如果启用 Guest 还是不能访问的请看：

1、默认情况下，XP 禁用 Guest 帐户
2、默认情况下，XP 的本地安全策略禁止 Guest 用户从网络访问
3、默认情况下，XP 的 本地安全策略 -> 安全选项里，"帐户：使用空密码用户只能进行控制台登陆"是启用的，也就是说，空密码的任何帐户都不能从网络访问只能本地登陆，Guest 默认空密码

所以，如果需要使用 Guest 用户访问 XP 的话，要进行上面的三个设置：启用 Guest、修改安全策略允许 Guest 从网络访问、禁用 3 里面的安全策略或者给 Guest 加个密码。

有时还会遇到另外一种情况：访问 XP 的时候，登录对话框中的用户名是灰的,始终是 Guest 用户，不能输入别的用户帐号。

原因是这个安全策略在作怪（管理工具 -> 本地安全策略 -> 安全选项 -> "网络访问：本地帐户的共享和安全模式"）。默认情况下，XP 的访问方式是"仅来宾"的方式，那么你访问它，当然就固定为 Guest 不能输入其他用户帐号了。

所以，访问 XP 最简单的方法就是：不用启用 Guest，仅修改上面的安全策略为"经典"就行了。别的系统访问 XP 就可以自己输入帐户信息

Chapter 8

VNN 文件网关使用介绍

Chapter
8

一．VNN文件加速网关简介

VNN-FAG（VNN File Acceleration Gateway）是美国 VNN 网络公司针对跨国和跨运营商进行大文件传输的应用需求开发的一款安全可靠的文件加速传送产品。该产品主要用于跨国和跨区域的企业，政府和金融行业的文件传输。

VNN-FAG 的工作原理是通过优化网络协议，解决跨国或跨运营商的带宽瓶颈，保证传送大的用户文件时，依然可以得到较大的有效带宽。VNN-FAG 内置多线程，分段校验和断点续传的功能，让用户在传送数 GB 的文件时，不用关心传送成功与否，保证文件可以快速安全可靠地传送到对方。

VNN-FAG 是一款网关形式的产品。在每一个办公地点，只需要部署一台网关。该办公地点的员工，都可以通过 IE 浏览器访问 VNN 文件网关的操作界面，在网关上指定接收文件目录和要将文件发送到哪一个远程文件网关。在文件被通过局域网传送到本地的 VNN 网关之后，用户就不用关心具体的文件的发送过程。被发送的文件将会从本地网关自动地发送到指定的远端网关。用户可以通过 VNN 网关界面来查询文件发送和接收的情况，包括已经发送和接收了多少文件，当前的文件发送速度等。

当文件被发送到目的网关后，该文件将会自动保存在预先指定的接收目录下面。对方的用户可以通过网络邻居，FTP 等方式，通过局域网获取该文件。

和一般的网络邻居比较，VNN 网关的文件传输速度会有 10 倍以上的提高。和 FTP 服务器比较，VNN 网关也有 3 到 10 倍的传输速度提高。以前存在的问题是使用一般文件传输方式传输速度太慢，并且对于几百兆以上的文件经常无法传送成功。利用 VNN 网关能够解决上述问题。例如，一般通过互联网，从中国发送一个大文件到美国，一般的 FTP 的速度可能平均在 10K 字节每秒，如果不支持断点续传那么很难发送成功。而使用 VNN 网关，传输速度可以达到 50～100 多 K 字节每秒。

Chapter 8

二. 当前常见大文件传送方法和缺陷

1. 作为邮件的附件发送
2. 使用 FTP 服务器
3. Windows 的网络邻居
4. 互联网上面的网络硬盘
5. 使用可以支持大附件的免费邮箱
6. 使用即时通讯软件 IM

存在的问题：

1. 作为邮件的附件发送

1） 通常邮箱对于文件的大小有限制。一般不能传送大于 10 兆的文件。如果要通过邮箱发送大文件给远端客户，即使对方邮箱空间很大，对方要成功接收大附件邮件也需要很长时间。常常会影响该用户的工作效率，并有可能影响此用户接收其它紧急邮件。
2） 普通邮件程序在发送邮件的过程中都是明文传递，这样附件中的文件内容有可能被骇客截取或者篡改，存有很大的安全隐患。
3） 在发送或接收大附件邮件的过程中,会极大影响远端或本地邮件服务器的邮件处理性能。
4） 大附件邮件将给邮件服务器的存储和备份工作带来很大负担。

2. 使用 FTP 服务器

1） FTP 的访问权限和文件目录控制需要由专人管理，如果设置不当极易引起机密文件的丢失和越权访问；
2） FTP 协议属于早期应用协议，在传送文件尤其是大文件时因为协议设计缺陷，导致文件传输效率不高，并且经常发生越传越慢的现象，一旦发生传输线路的中断，往往要对大文件重新传送；
3） FTP 协议对传输的文件无加密措施，在互联网上进行文件的明文传输存在很大安全隐患。

3. Windows 的网络邻居

1) 网络邻居使用的是 Samba 协议，该协议为在局域网传送文件而设计，当在互联网上面使用它进行文件传输时，速度非常慢；
2) 对于有些公司不同部门之间，每天需要传送数 GB 的文件（软件升级版本，光盘镜像，数据库备份数据和多媒体文件等）。这些传送的文件分散在多个共享文件夹中，这些文件是否需要保留网管人员无从知晓，造成了硬盘空间的极大浪费；
3) 保密性不高，使用文件共享服务器，全部文件都保存在共享目录里，很难进行访问权限的控制；
4) 两端局域网如果通过网络邻居共享文件，非常容易引起病毒跨局域网的交叉感染。

4. 网络硬盘

1) 文件没有经过保密处理就保存在服务商的服务器上，对网络硬盘服务商来说完全透明，对于商业用户来讲从文件的保密性和隐私性角度来考虑无法接受此服务方式；
2) 很难做精细的用户访问权限控制，只要非法用户扫描到该文件资源链接，极有可能造成文件被他人拷贝浏览；
3) 如果跨 ISP 运营网络访问此网络硬盘服务器，文件传输速度很慢；如果大量用户同时进行文件的上传下载，网络磁盘服务器的资源如果不够健壮，也将导致文件传输速度缓慢；
4) 一般单个文件，不能超过 1GB。网络硬盘服务商对所存储的文件有严格的大小限制。

5. 免费邮箱

1) 对服务商来讲邮件附件内容是透明的，存在保密性隐私性缺陷；
2) 对企业用户来讲非常容易造成公司核心机密文件的泄露和丢失；
3) 免费邮箱服务器的带宽资源有限，在附件下载上传过程中速度不快。

6. 通过聊天软件 IM

1) 需要双方同时上网在线；
2) 传送文件不加密；
3) 不支持断点续传；
4) 远距离传送文件速度很慢；
5) 很多大型公司和企业禁止员工在上班时间使用聊天软件；
6) 网络管理员很难进行文件传送的统一管理和维护。

Chapter 8

三．VNN文件加速网关功能

1. 自动发送文件（使用智能的人性化界面）

2. 文件在互联网上面加密传送（文件在公网传输的安全性）

3. 自动将大文件分片，自动校验，在接收端自动合并（分割传送）

4. 如果将一个大文件发送到多个地点，自动采用 P2P 的原理，获取更大的带宽。

5. 一个办公地点，只需要配备一台网关，其它的用户只需要从自己的电脑上面使用一般的浏览器就可以，不用安装任何客户端软件。

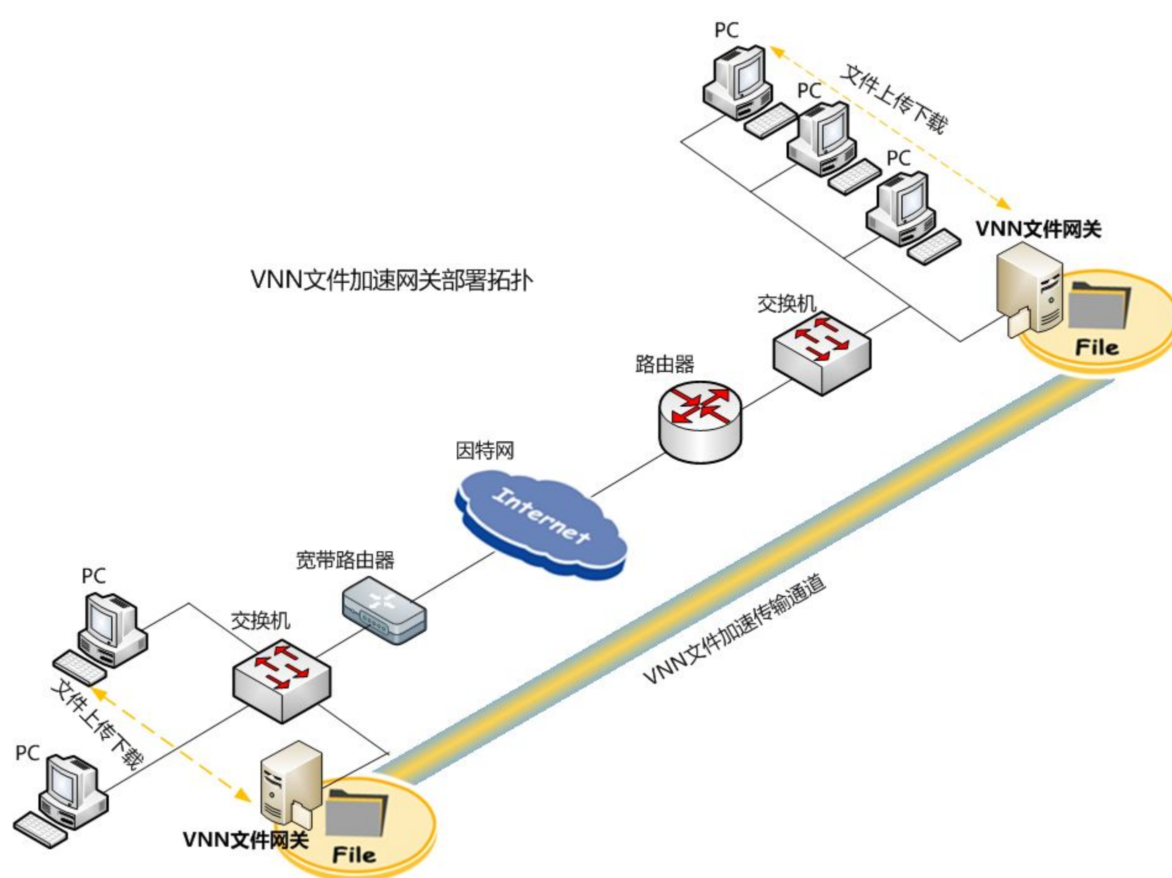
6. VNN 网关可以部署在用户的局域网里面，不用在防火墙或路由器上面做复杂配置，也无需为其配置固定公网 IP，只要保证 VNN 网关能够访问因特网。如果不同的办公地点已经使用 VPN 互相联通，VNN 网关的数据可通过该 VPN 隧道传送。如果没有配置 VPN，就采用 VNN 的加密隧道传送。

7. 网管可以对文件网关的传输访问权限进行集中控制。

8. VNN 网关有软件和硬件两种产品形式。本用户说明介绍的是软件形式。

Chapter 8

四．VNN文件加速网关部署拓扑



Chapter 8

五．VNN文件加速网关部署步骤

1. 在每一个需要使用 VNN 网关的办公地点，选择一台具有静态 IP 地址的电脑安装 VNN 网关软件，作为 VNN 文件加速网关(**VNN 文件加速网关的 IP 地址必须为固定 IP，以方便局域网其他用户进行访问)。

2. 该电脑可以是任何 P4 以上的 CPU，内存不小于 1GB。运行 Windows XP，Windows 2003 或 Windows Vista。

3. VNN 网关的接收目录，可以使用电脑内置的硬盘或通过网络邻居使用其它文件服务器上面的空间。接收到的文件会被自动存放到这个目录。用户可以通过网络邻居共享文件夹的访问方式从该目录获取文件。

4. 安装 VNN 文件加速网关软件：如上页文件网关部署拓扑图所示，在需要安装 VNN 文件加速网关的 PC 或者服务器上双击 VNN4EntSetup32.exe 安装文件，开始 VNN 文件加速网关的安装，在安装过程中点击“NEXT”按钮，安装成功后将在桌面右下角系统通知区域出现图标表示安装运行成功，可以进行下一步的 VNN 文件加速网关配置工作。

Chapter 8

六．VNN文件加速网关的配置

1. 登录 VNN 网络：

在 VNN 文件加速网关主机上使用 VNN 帐号登录(申请 VNN 帐号步骤请参见 VNN 使用说明书第二章)，登录成功后 VNN 文件网关将获得一个唯一的与 VNN 帐号绑定的虚拟 IP 地址，同时对端 VNN 文件加速网关主机登陆后也将获得一个唯一的 VNN IP 地址，两端文件网关将使用这两个 VNN IP 进行文件加速传输。

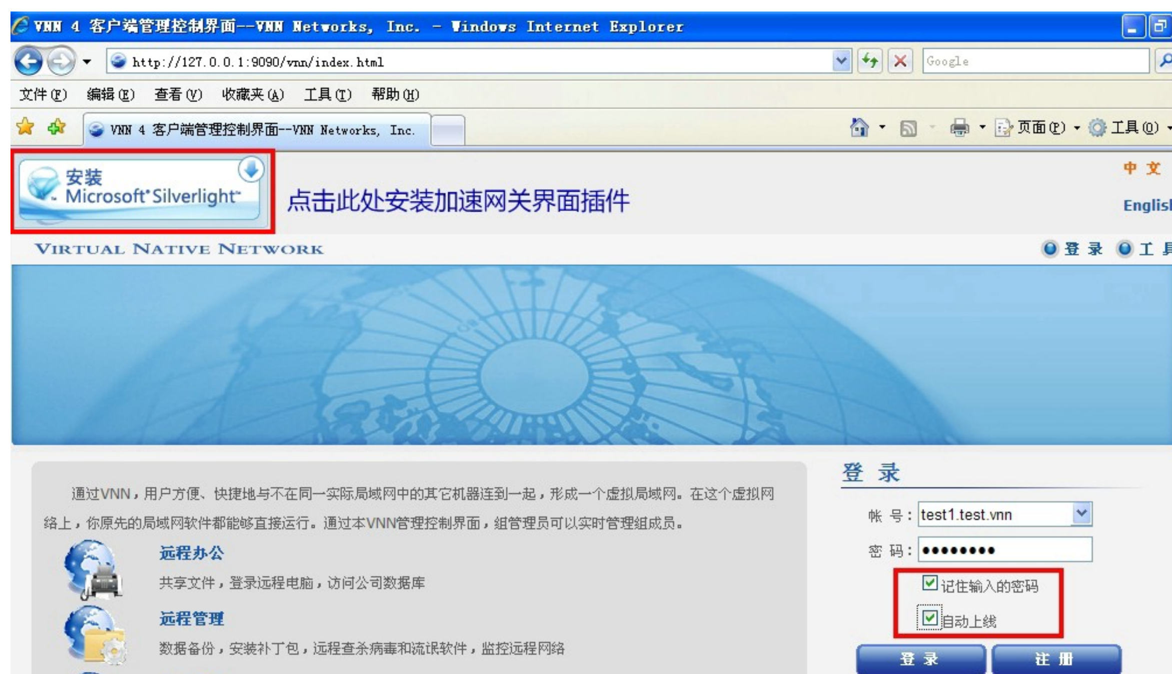
VNN 网络登录步骤：

VNN文件加速网关安装后将自动打开一个浏览器界面让用户进行登录（您也可以在安装了VNN文件加速网关的主机中打开IE，在浏览器里敲入：http://localhost:9090/，回车后将出现如下界面：



2. 安装 Silverlight 插件

点击“GO”按钮出现 VNN 登录界面，如下图所示：



- 界面左上角提示安装 Microsoft Silverlight 插件，VNN 文件加速网关操作界面需要使用此插件，所以请在提示图片上点击下载安装此插件；

- 使用 test1.test.vnn 帐号进行登录，(**注意此处为示例，使用时请使用实际帐号登录)，并且设置为记住输入的密码和自动上线。这样可以保证每次文件网关电脑启动之后都迅速进入正常工作状态。登录后出现 VNN 软件使用首界面(远端文件网关以 XX.test.vnn 帐号进行登录**此处为示例)，如下图所示：



3. 进入 VNN 文件加速网关的配置界面

在 VNN 软件使用界面菜单中点击“应用”，在出现的界面中点击“VNN 文件加速网关”，如下图所示：



4. 开始配置 VNN 文件加速网关

在出现的 VNN 文件加速网关配置界面上点击“设置”按钮，进入具体配置界面：



5. 配置 VNN 文件加速网关的两个基本参数

- 默认保存路径——指定本网关接收文件的保存目录
- 自动发送对端——指定本网关可向哪些对端网关发送文件



实际操作：

- **默认保存路径**：点击“浏览”按钮可以选择一个目录用来保存对端文件网关发过来的文件，此处建议选择非系统盘（C 盘）的另外一个盘符目录来保存对端发送过来的文件，并且此磁盘分区有足够空间可以保存对方发送过来的大文件。
- **自动发送对端**：在要发送文件给对端的文件网关标识前面打“√”确认。
- **描述**：可在文件网关目录中的“描述”一栏中填写对端文件网关的中英文标识名称，以方便用户在传送文件前更加明确文件传送的目的地。

配置完成以上步骤后请点击“确定”按钮完成 VNN 文件加速网关的设置，下面介绍如何给远端文件网关发送文件。

Chapter 8

七．使用VNN文件加速网关进行文件传输

1. 在文件网关上发送接收文件

启动IE浏览器，键入 http://localhost:9090/vnn/v2v/ 地址，将出现VNN文件加速网关的首界面，如下图所示：



发送文件界面右上端的下拉框可进行中英文语言的切换

- “发送文件”选项卡可进行文件发送操作；
- “查看状态”选项卡可查看文件发送的状态及结果。



- 进行文件发送操作：

点击“新增文件”按钮，如下图所示：



- 选择发送文件的目标对端：



点击上图“选择文件”按钮选取文件后即可迅速向对端发送发件，并且可以在“发送文件”选项卡中查看文件发送状态。



- **查看文件发送状态**

本端用户和对端用户也可以在 VNN 文件加速网关界面的“查看状态”选项卡中查看文件发送状态，如下图所示：

文件加速网关　中文

发送文件　查看状态

传送完成的文件　正在接收的文件

文件名	传输状态	对端IP	大小	总计用时	平均速度	开始时间	结束时间	已完成	文件路径
welcome.png	发送失败	2.1.219.62	0	00:00:00	B/s	13:32:59	13:32:59	0	D:\V2VTest\receive\SubnetUpload\127.0.
用友公司地图UFIDA1.png	发送失败	2.1.220.59	0	00:00:00	B/s	13:33:55	13:33:55	0	D:\V2VTest\receive\SubnetUpload\127.0.
用友公司地图UFIDA1.png	发送完成	2.2.41.246	758.6KB	00:00:15	50.57KB/s	13:33:58	13:34:13	758.6KB	D:\V2VTest\receive\SubnetUpload\127.0.
BOBO-光荣.mp3	接受完成	2.1.149.10	5.1MB	00:00:09	580.27KB/s	13:53:02	13:53:11	5.1MB	D:\V2VTest\receive\receive\2.1.149.10\1
try - 勇敢的女孩.mp3	接受完成	2.1.149.10	3.6MB	00:00:07	526.63KB/s	13:54:06	13:54:13	3.6MB	D:\V2VTest\receive\receive\2.1.149.10\1

2.　在局域网的主机上使用文件网关发送和获取文件

如果需要从其他主机上访问本地文件网关进行文件传输操作，您首先需要进行如下设置

- **打开 VNN 文件网关的局域网访问功能：**

首先在安装了VNN文件加速网关的主机上打开IE敲入http://localhost:9090/vnn/index.html进入VNN登录界面，如下图所示



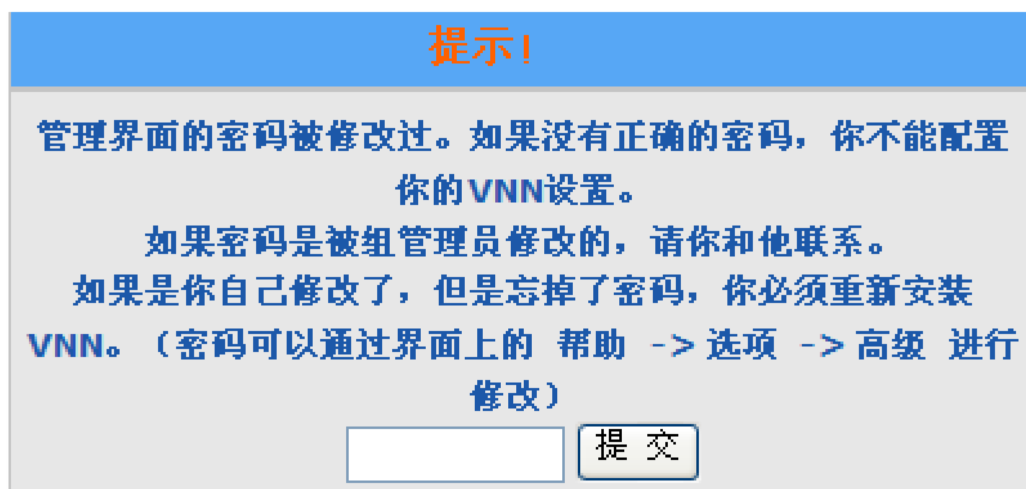
Chapter 8

点击“工具”按钮在出现的界面中点击“选项”--> “高级”，打开“远程控制管理”，将“允许远程控制管理”选项打勾，输入管理密码后点击“保存”按钮（如下图所示）



完成以上步骤后你就可以在局域网的其他主机上启动IE浏览器敲入 http:// 文件网关IP:9090/vnn/v2v/ 地址，进入VNN文件加速网关的发送文件界面进行操作，发送文件的步骤与在文件网关上发送文件的步骤一样（请参见上面在文件网关上发送文件的说明）。

**注意：经过上面设置后如果今后需要在 VNN 文件网关上登录 VNN 软件使用界面也必须输入上面设置的远程控制管理密码，如下图所示：



- 从文件网关获取文件：

如果在文件网关界面中文件传输状态显示已经“接收完成”，本地局域网用户就可以通过网络邻居共享文件夹的方式进入文件网关的接收文件夹下载所需文件。如下图所示，此处 10.99.99.207 为本地 VNN 文件加速网关的 IP 地址，VNN-Receive 为文件网关接收文件夹的共享文件夹名称：

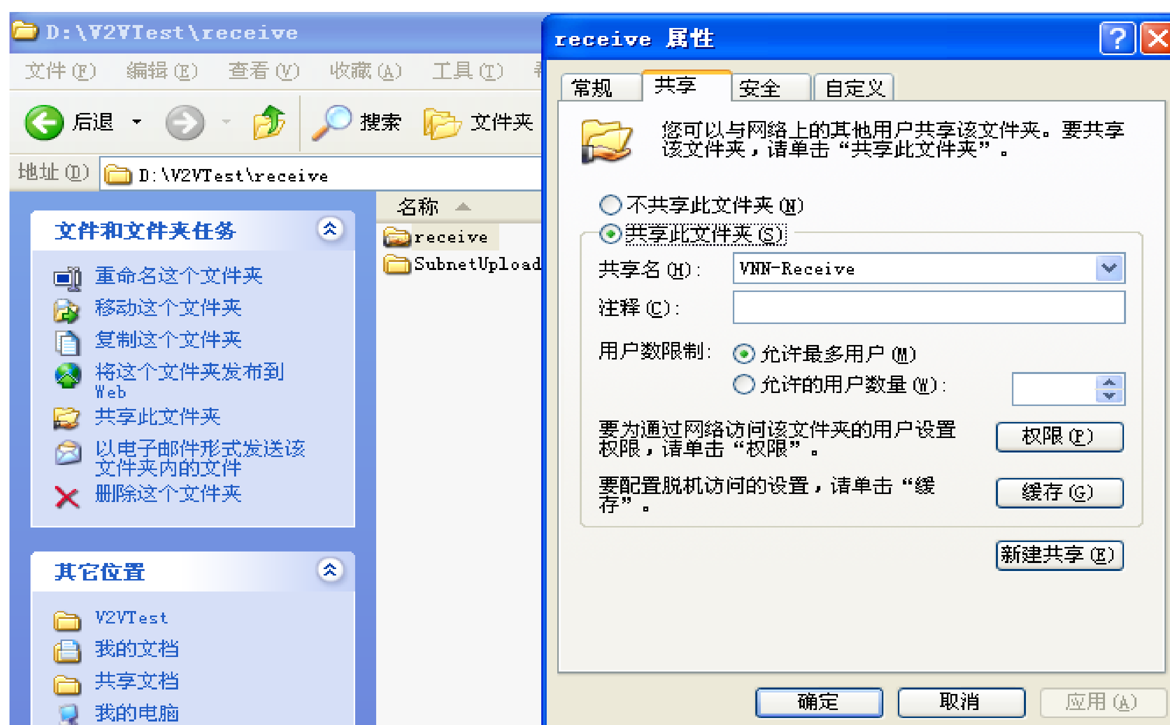


辅助设置——在 VNN 文件网关上设置接收文件夹的远程访问共享

在需要共享的文件夹上点击鼠标右键，点击“共享和安全”，如下图所示



在出现的窗口中点击“共享此文件夹”选项，在共享名中填入此文件夹的共享标识，如下图所示

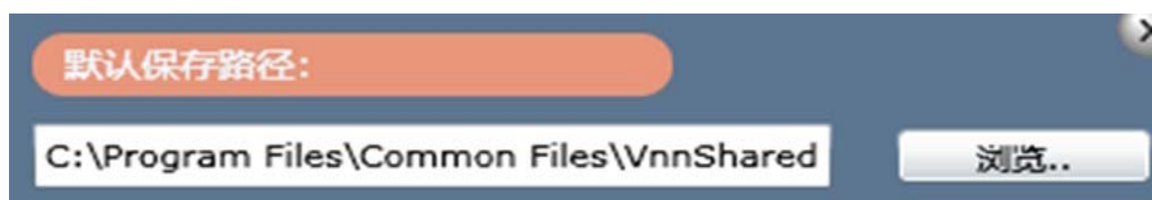


Chapter 8

八. 使用注意事项

1. 关于默认接收文件夹：

如果没有对本地网关接收文件夹进行更改设定（第五部分第（4）节）



那么默认的本地网关接收文件夹是 C:\Program Files\Common Files\VNNShared\VNN Core Engine Service\receive\2.2.132.235\127.0.0.1（注意 VNN IP 有所不同）



**强烈建议将此保存文件目录修改成非系统磁盘目录并具有较大存储空间的磁盘目录。

2. 关于发送端发送文件成功后的文件处理：

通过本地文件网关给其他文件网关成功发送文件后，如果此文件无再次向其他网关传输的可能，建议在本地文件网关上删除已发送过的文件以节省硬盘空间 C:\Program Files\Common Files\VNNShared\VNN Core Engine Service\SubnetUpload
如果修改过默认接收文件夹，则此文件夹格式为：指定的接收文件夹\SubnetUpload

3. 关于文件网关的 IP 地址：

为了让同一个办公地点的用户可以通过浏览器访问文件网关，需要配置该网关 IP 地址为固定 IP 地址。

4. 请使用 IE 浏览器访问文件网关操作界面

Chapter 9

发布应用

当您登录普通帐号后，即可在看到下图中的界面。

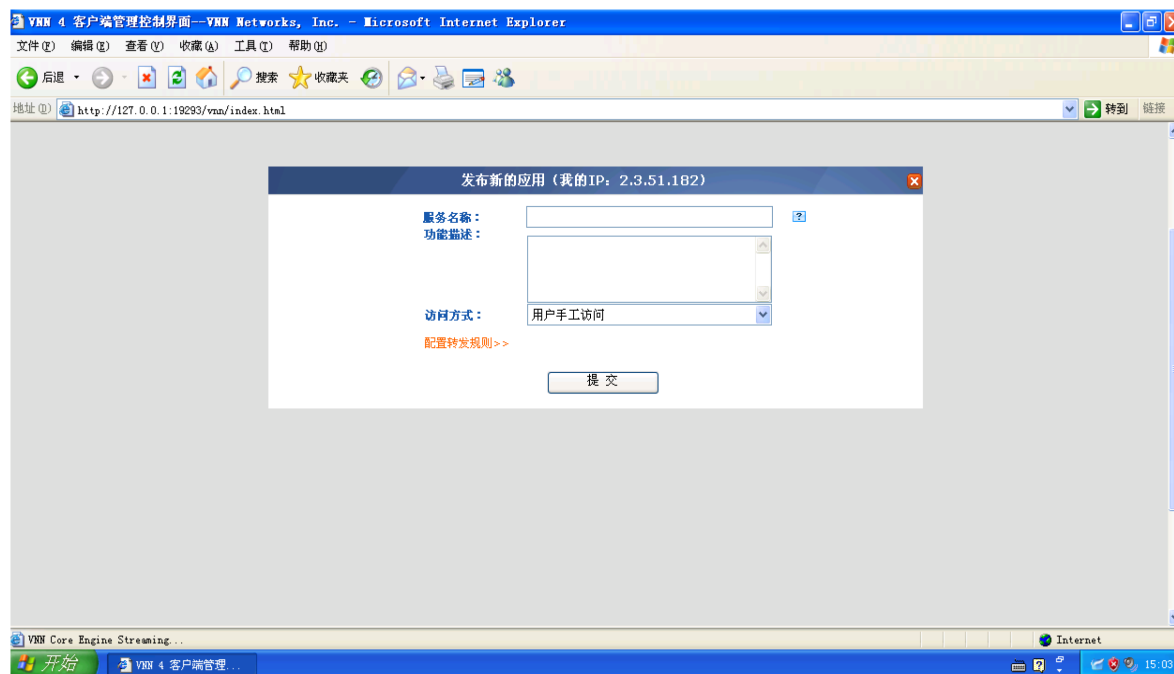


通过点击应用发布对话框右上角的小红叉即可看到登录后的应用界面。



这就是 VNN 的标准登录界面，在界面中您可以查看、访问或配置各种功能和应用。

通过点击上图中右上角的“发布新应用”按钮后即可看到应用发布界面（如下图）



Chapter 9

VNN 的发布应用分为三种方式（即访问方式中的选项）

第一种是 Web 应用，需要有 Web 服务器，或者有一个 VNN 的网关或端口映射到这台 Web 服务器。

第二种是远程桌面，即通过远程桌面方式访问特定的 VNN 帐号，或端口映射、VNN NAT 网关后的计算机。

第三种则是特定的应用程序发布，即发布用户当前计算机的应用到 VNN 上，远程计算机必须安装该应用程序。
通过选择对应的方式即可做到对应的应用发布。我们在这儿举例说明：

第一种：

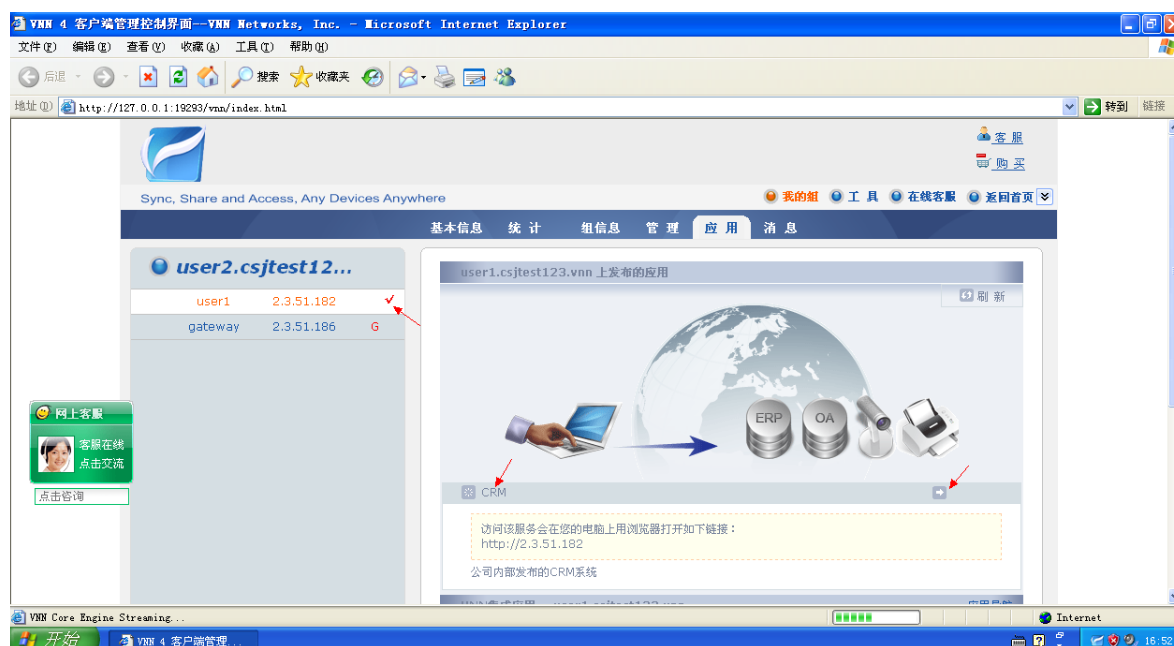
企业内部有一台基于 B/S（浏览器 / 服务器）架构的 CRM 系统。

如果是这种现象，您首先需要在服务器上安装 VNN 的客户端，然后登录界面，并且按照下图发布如下应用：

请注意：上图中的 http://2.3.51.182 是本教程的举例，您需要在服务器上进行操作时替换成服务器上的实际 VNN 的 IP 地址和路径。

当您在服务器上完成以上的操作后，在客户端登录同组的其他帐号，比如服务器上登录的是 user1，那么客户端可以登录 user2。

登录后，在左侧界面点击服务器的帐号，然后在右侧点击所发布的 CRM 应用，即可看到发布成功的 CRM 系统。



第二种：

企业内有一台需要远程管理的 Windows Server 2003 服务器，只需要开启 Windows Server 2003 自带的远程桌面，然后在“添加新应用中”，按照下图进行配置即可：

发布新的应用（我的IP：2.3.51.182）

服务名称：远程管理公司服务器

功能描述：

访问方式：客户端自动启动下面指定的远程桌面命令

命令行：mstsc.exe /v:2.3.51.182　测试

示　例：mstsc.exe /v:2.3.51.182:3389

配置转发规则>>

提 交

请注意：上图中的 2.3.51.182 为本教程的举例，在实际部署时请填写服务器上的实际 VNN 的 IP 地址。

当您在服务器上完成以上的操作后，在客户端登录同组的其他帐号，比如服务器上登录的是 user1，那么客户端可以登录 user2。

登录后，在左侧界面点击服务器的帐号，然后在右侧点击所发布的远程桌面应用，将会自动出现远程桌面连接对话框，连接上后即可。

第三种：

企业有一台财务软件，支持通过命令行方式指定服务器地址（类似： Shell.exe -ip 192.168.0.2），并且在客户端安装了该软件的情况下，可以通过以下配置来访问该应用。

发布新的应用（我的IP：2.3.51.182）

服务名称：XX财务软件
功能描述：
访问方式：客户端自动启动下面指定的命令行
命令行：C:\XX财务软件\Shell.exe -ip:2.9.51.182　测试
示 例：C:\WINDOWS\system32\ping.exe -t g.cn
配置转发规则>>
提 交

请注意：上图中的 2.3.51.182 IP 地址和具体的连接是为本教程的举例，在实际部署时请填写服务器上的实际 VNN 的 IP 地址，和客户端上安装的软件路径。

登录后，在左侧界面点击服务器的帐号，然后在右侧点击所发布的应用程序，将会自动执行对应的程序，并且向程序传递对应的 IP 地址参数。

高级应用：

VNN 的发布应用功能中还集成了端口转发功能，如果您需要独立转发一个端口，那么您必须发布一个访问方式为“用户手工访问”的应用。如果是 Web 服务，则可以选择“客户端自动用浏览器打开下面的 URL”的访问方式。

比如您有这样的需求，公司内部有一台基于 Linux 的 Apache Web 服务器，无法安装 VNN，但是需要通过 VNN 远程异地访问，那么，在该服务器所在的局域网中的一台 Windows 计算机中安装并且登录 VNN，然后，在“添加新应用”中点击“配置转发规则”连接，即可看到配置转发的界面。

假设该服务器的地址为 192.168.1.2 ，端口为默认的 80，那么按照以下设置即可：

发布新的应用（我的IP：2.3.51.182）

服务名称：转发到Web服务器
功能描述：
访问方式：客户端自动用浏览器打开下面的URL
URL：http://2.3.51.182 测试
示　例：http://2.3.51.182/erp/
客户端自动通过如下代理访问上面的URL

配置转发规则>>

端口转发将到(IP1, PORT1)的访问转为到(IP2, PORT2)的访问。当访问IP1:PORT1时，就像访问IP2:PORT2一样。
转发规则　添 加　全部规则列表

地址	端口	转发目的地址	转发目的端口	
0.0.0.0	80	192.168.1.2	80	删 除

提 交

注意：本例中的 2.3.51.182 和 192.168.1.2 这些 IP 地址完全是为本教程的举例，在实际部署时请填写服务器的实际地址和当前 VNN 的 IP 地址。

同时，由于 VNN 内建了 Socks 代理，对于特殊的 Web 页面，如页面中存在绝对连接，无法通过端口映射解决的，只需要启用 VNN 内建的 Socks 代理即可（如下图）

发布新的应用（我的IP：2.3.51.182）

服务名称：转发到Web服务器

功能描述：

访问方式：客户端自动用浏览器打开下面的URL

URL：http://2.3.51.182 测试

示 例：http://2.3.51.182/erp/

客户端自动通过如下代理访问上面的URL

HTTP代理 SOCKS代理 VNN内置代理

本地VNN地址：2.3.51.182

本地VNN端口：2387

配置转发规则>>

端口转发将到(IP1, PORT1)的访问转为到(IP2, PORT2)的访问。当访问IP1:PORT1时，就像访问IP2:PORT2一样。

转发规则 添 加 全部规则列表

地址	端口	转发目的地址	转发目的端口

提 交

通过启用代理，当客户端通过该帐号的 VNN 所发布的 Web 应用访问，将全部通过这台计算机进行转发，通过应用发布界面的浏览器能够自动的配置好 VNN 的内建代理。

注意：客户端只有通过 VNN 内置的应用发布平台打开的浏览器才具备代理功能，通过该浏览器打开的新窗口也能够正确的使用代理。但是独立打开浏览器窗口将不具备该功能。同时，该功能只支持 IE 浏览器的自动配置，其他浏览器，诸如 Firefox 需要手动配置。

技术支持联系方式



客服电话：

010-58731939 805/806

010-58731163 805/806

010-58731165 805/806

传真：

010-58733132

邮箱：

support@bizvnn.com

网站：

http://www.vnn.cn